

# One-Shot Decoupling

Frédéric Dupuis\*

Mario Berta\*

Jürg Wullschleger<sup>†,‡</sup>

Renato Renner\*

\*Institute for Theoretical Physics  
ETH Zurich, Switzerland

<sup>†</sup>Department of Computer Science and Operations Research  
Université de Montréal, Quebec, Canada

<sup>‡</sup>McGill University, Quebec, Canada

## Abstract

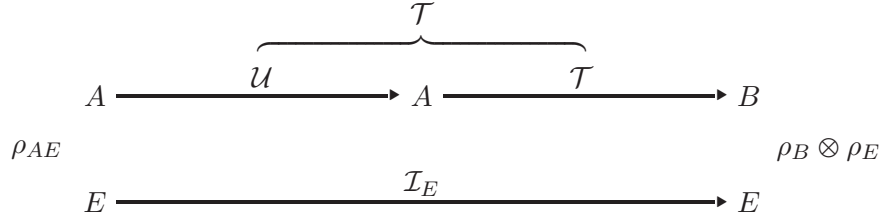
If a quantum system  $A$ , which is initially correlated to another system,  $E$ , undergoes an evolution separated from  $E$ , then the correlation to  $E$  generally decreases. Here, we study the conditions under which the correlation disappears (almost) completely, resulting in a *decoupling* of  $A$  from  $E$ . We give a criterion for decoupling in terms of two smooth entropies, one quantifying the amount of initial correlation between  $A$  and  $E$ , and the other characterizing the mapping that describes the evolution of  $A$ . The criterion applies to arbitrary such mappings in the general one-shot setting. Furthermore, the criterion is tight for mappings that satisfy certain natural conditions. Decoupling has a number of applications both in physics and information theory, e.g., as a building block for quantum information processing protocols. As an example, we give a one-shot state merging protocol and show that it is essentially optimal in terms of its entanglement consumption/production.

## 1 Introduction

Correlations in quantum systems, and in particular entanglement, have been in the focus of (both theoretical and experimental) research in quantum information science over the past decades. As a result, one has nowadays a pretty good (although still not complete) understanding of quantum correlations and, in particular, the processes that create them. In this work, we take—so to speak—an opposite approach and study conditions under which two systems can be decoupled, i.e., brought to a state where they are uncorrelated.

We call a system,  $B$ , *decoupled* from another system,  $E$ , if the joint state of the two systems,  $\rho_{BE}$ , has product form  $\rho_B \otimes \rho_E$ . Operationally, this means that the outcome of any measurement on  $B$  is statistically independent of the outcome of any measurement on  $E$ . Or, in information-theoretic terms, the system  $E$  does not give any information on  $B$  (and can therefore safely be ignored when studying  $B$ ).

**Decoupling Theorem.** Our goal is to characterize the conditions under which the evolution of a system results in decoupling. For this, we consider a system,  $A$ , that may



**Figure 1: Decoupling.** The initial system,  $A$ , may be correlated to a reference system  $E$ . The evolution is modeled as a mapping  $\bar{\mathcal{T}}$  from  $A$  to  $B$ . The final state of  $B$  is supposed to be independent of  $E$ . The subdivision of  $\bar{\mathcal{T}}$  into a unitary  $\mathcal{U}$  and a mapping  $\mathcal{T}$  is required for the formulation of our decoupling criterion.

initially be correlated to  $E$ . Furthermore, we assume that the system  $A$  undergoes an evolution, described by a TPCPM<sup>1</sup>  $\bar{\mathcal{T}}$  from  $A$  to  $B$ , during which no interaction with  $E$  takes place (see Fig. 1). The main result of this work is a decoupling theorem, i.e., a criterion that provides necessary and sufficient conditions for decoupling (of  $B$  from  $E$ ). The criterion depends on two entropic quantities, characterizing the initial state,  $\rho_{AE}$ , and the mapping  $\bar{\mathcal{T}}$ , respectively.

The decoupling criterion can be conceptually split into two parts, called *achievability* and *converse* part, which we now describe informally. The full technical statements are provided as Theorems 3.1 and 4.1 in Sections 3 and 4, respectively. For their formulation, it is convenient to view  $\bar{\mathcal{T}}$  as a sequence,  $\bar{\mathcal{T}} = \mathcal{T} \circ \mathcal{U}$ , where  $\mathcal{U}$  is an arbitrary unitary on  $A$ , and  $\mathcal{T}$  a fixed TPCPM from  $A$  to  $B$ .

*Achievability:* Decoupling is achieved for most choices of  $\mathcal{U}$  if  $H_{\min}^{\varepsilon}(A|E)_{\rho} + H_{\min}^{\varepsilon}(A|B)_{\tau} \gtrsim 0$ .

*Converse:* Decoupling is not achieved for any choice of  $\mathcal{U}$  if  $H_{\min}^{\varepsilon}(A|E)_{\rho} + H_{\max}^{\varepsilon}(A|B)_{\tau} \lesssim 0$ .

The criteria refer to the *smooth min- and max-entropies* introduced in [RW04, Ren05], which can be seen as generalizations of the von Neumann entropy (cf. Section 2 for definitions and properties). The smooth min-entropy  $H_{\min}^{\varepsilon}(A|E)_{\rho}$  is a measure for the correlation present in the initial state  $\rho_{AE}$  — the larger this measure, the less dependent is  $A$  on  $E$  (see Table 1 for some typical examples). The quantities  $H_{\min}^{\varepsilon}(A|B)_{\tau}$  (for the achievability) and  $H_{\max}^{\varepsilon}(A|B)_{\tau}$  (for the converse) measure how well the mapping  $\mathcal{T}$  conserves correlations. Roughly, they quantify the uncertainty one has about a “copy” of the input,<sup>2</sup>  $A$ , given access to the output,  $B$ , of  $\mathcal{T}$  (cf. Table 2). We note that the expressions for the achievability and for the converse essentially coincide in many cases of interest (see the discussion in Section 4).

As a typical example, consider  $m$  qubits,  $A$ , that are classically maximally correlated to  $E$  (so that  $H_{\min}^{\varepsilon}(A|E) = 0$ , cf. second row of Table 1). Furthermore, assume that  $A$  undergoes a reversible evolution,  $\mathcal{U}$ , after which we discard  $m - m'$  qubits, corresponding to a partial trace,  $\mathcal{T} = \text{Tr}_{m-m'}$  (see last example of Table 2). Our criterion then says that the remaining  $m'$  qubits will, for most evolutions  $\mathcal{U}$ , be decoupled from  $E$  whenever  $m' < m/2$ . Conversely, if this condition is not satisfied, some correlation will necessarily be retained.

<sup>1</sup>A *Trace-Preserving Completely-Positive Map* (TPCPM) is a linear function that maps density operators to density operators.

<sup>2</sup>More precisely, the entropy is evaluated for the state  $\tau_{AB}$  obtained by applying  $\mathcal{T}$  to one half of an entangled state.

Description of initial state	$\rho = \rho_{AE}$	$H_{\min}^\varepsilon(A E)_\rho$
$k$ random bits $A$ independent of $E$	$2^{-k} \mathbb{1}_A \otimes \rho_E$	$k$
$k$ bits $A$ correlated classically to $E$	$2^{-k} \sum_{i=1}^{2^k}  i\rangle\langle i _A \otimes  i\rangle\langle i _E$	0
$k$ qubits $A$ fully entangled with $B$	$ \Psi\rangle\langle\Psi $ , where $\Psi = 2^{-k/2} \sum_{i=1}^{2^k}  i\rangle_A \otimes  i\rangle_E$	$-k$

**Table 1: Dependence on the initial state.** The table illustrates how the term  $H_{\min}^\varepsilon(A|E)_\rho$  (for  $\varepsilon \rightarrow 0$ ) in the decoupling criterion depends on the initial state  $\rho_{AE}$ . In all three examples,  $A$  is assumed to be a  $k$ -qubit system with orthonormal basis  $\{|i\rangle_A\}_{i=1}^{2^k}$ . Similarly,  $\{|i\rangle_E\}_{i=1}^{2^k}$  is an orthonormal family of states on  $E$ .

**Applications.** The notion of decoupling has various applications in information theory and in physics. Many of these applications have in common that decoupling of a system  $B$  from a system  $E$  is used to show that  $B$  is maximally entangled with a complementary system,  $R$ . Indeed, under the assumption that  $R$  is chosen such that the joint state,  $\rho_{BER}$ , is pure,  $\rho_{BE} = \rho_B \otimes \rho_E$  immediately implies that there exists a subsystem  $R'$  of  $R$  such that the state on  $\rho_{BR'}$  is pure. If, in addition,  $\rho_B$  is fully mixed,  $\rho_{BR'}$  is necessarily maximally entangled.

In the context of information theory, this type of argument is, for example, used to analyze *state merging* [HOW05, HOW07], i.e., the task of conveying a subsystem from a sender to a receiver — who already holds a possibly correlated subsystem — using classical communication and entanglement. Another example, where decoupling is used in a similar fashion, is the *Quantum Reverse Shannon Theorem* [BSST02, BDH<sup>+</sup>09, BCR11]. In fact, the proof of this theorem given in [BCR11] refers to a coherent form of state merging (also known as the *Fully Quantum Slepian Wolf* or *Mother Protocol* [ADHW09]) where the classical communication is replaced by quantum communication. Decoupling can also be used for the characterization of correlation and entanglement between systems, erasure processes, as well as channel capacities (see, e.g., [GPW05, Bus09, HHWY08]). In addition, its classical analogue, *Privacy Amplification* [BBCM95, RK05], is widely used in classical and quantum cryptography.

Decoupling processes are also crucial in physics. For example, the evolution of a thermodynamical system towards thermal equilibrium can be understood as a decoupling process, where the system under consideration decouples from the observer (somewhat analogous to the considerations in [LPSW09, Par89a, Par89b]). Recent work indeed suggests that there is a close relation between smooth entropies and quantities that are relevant in thermodynamics [DRRV09, dRAR<sup>+</sup>11]. Similarly, black hole radiation may be analyzed from such a point of view [HP07, BP07, BZ09].

**History and Related Work.** While various standard results in quantum information theory have been proved using ideas related to decoupling, the concept came into its own with the discovery of *State Merging* protocols [HOW05, HOW07] and, later, the *Fully Quantum Slepian Wolf* protocol [ADHW09]. These are based on specific decoupling processes where the mapping  $\mathcal{T}$  is either a projective measurement or a partial trace. In this

Description of mapping	$\mathcal{T}$	$H_{\min}^\varepsilon(A B)_\tau$
identity on $m$ qubits	$\sigma \mapsto \sigma$	$-m$
orthogonal measurement on $m$ qubits	$\sigma \mapsto \sum_{i=1}^{2^m}  i\rangle\langle i  \sigma  i\rangle\langle i $	$0$
erasure of $m$ qubits	$\sigma \mapsto \text{Tr}(\sigma)  0\rangle\langle 0 $	$m$
identity on $m'$ , orthogonal measurement on $m - m'$ qubits	$\sigma \mapsto \sum_{i=1}^{2^{m-m'}} (\mathbb{1}_{m'} \otimes  i\rangle\langle i ) \sigma (\mathbb{1}_{m'} \otimes  i\rangle\langle i )$	$-m'$
identity on $m'$ , erasure on $m - m'$ qubits	$\sigma \mapsto \text{Tr}_{m-m'}(\sigma)$	$m - 2m'$

**Table 2: Dependence on the mapping.** The table illustrates how the term  $H_{\min}^\varepsilon(A|B)_\tau$  (which in these examples coincides with  $H_{\max}^\varepsilon(A|B)_\tau$ ) in the decoupling criterion depends on the mapping  $\mathcal{T}$ . In all five examples, the input space,  $A$ , is assumed to consist of  $m$  qubits with orthonormal basis  $\{|i\rangle_A\}_{i=1}^{2^m}$ . The last two examples have a smaller output space consisting of only  $m'$  qubits. The penultimate one can be seen as a combination of the first and the second, and the last one can be seen as a combination of the first and the third. (The smooth min-entropies are evaluated for  $\varepsilon \rightarrow 0$ .)

early work, the decoupling was analyzed in terms of the dimensions of certain subsystems (rather than smooth entropies).

These decoupling results have been generalized in [WR09, Ber08] to include mappings  $\mathcal{T}$  that consist of combinations of projective measurements and partial traces. Furthermore, in this work, the criterion has been expressed in terms of smooth entropies. Independently of this, a general decoupling theorem that can be applied to any type of mapping has been developed [Dup09]. This result is essentially (up to the use of different entropy measures) equivalent to Theorem 3.1 presented here. We also note that the aforementioned characterizations of decoupling can be seen as special cases of this general result.

The above work was mostly concerned with achievability. Converse results were so far only known in special cases. In particular, in [BRW07] and [Ber08] (see also [Ren09]) converse theorems have been derived for the case where the mapping  $\mathcal{T}$  is a projective measurement. The converse theorem presented here, Theorem 4.1, generalizes these results.

**Structure of the Paper.** In Section 2 we introduce the notation and review the definitions and main properties of the entropy measures used in this work. Our main achievability result for decoupling is given in Section 3, whereas Section 4 contains a converse that is tight in many cases of interest. The use of the decoupling technique is illustrated in Section 5, where we show how to obtain optimal one-shot quantum state merging. We conclude with a discussion in Section 6.

## 2 Preliminaries

### 2.1 Notation

We denote the Hilbert space associated to a system  $A$  by  $\mathcal{H}_A$ . We only consider finite-dimensional systems and denote the dimension of  $\mathcal{H}_A$  by  $|A|$ . The set of linear operators on  $\mathcal{H}$  is denoted by  $\mathcal{L}(\mathcal{H})$  and the set of nonnegative operators on  $\mathcal{H}$  by  $\mathcal{P}(\mathcal{H})$ . We define the sets of subnormalized states  $\mathcal{S}_{\leq}(\mathcal{H}) = \{\rho \in \mathcal{P}(\mathcal{H}) : \text{Tr } \rho \leq 1\}$  and normalized states  $\mathcal{S}_=(\mathcal{H}) = \{\rho \in \mathcal{P}(\mathcal{H}) : \text{Tr } \rho = 1\}$ .

The tensor product of  $\mathcal{H}_A$  and  $\mathcal{H}_B$  is denoted by  $\mathcal{H}_{AB} \equiv \mathcal{H}_A \otimes \mathcal{H}_B$ . For multipartite operators  $\rho_{AB} \in \mathcal{P}(\mathcal{H}_{AB})$ , we write  $\rho_A = \text{Tr}_B(\rho_{AB})$  for the corresponding reduced operator. For  $M_A \in \mathcal{L}(\mathcal{H}_A)$ , we write  $M_A \equiv M_A \otimes \mathbb{1}_B$  for the enlargement on any  $\mathcal{H}_{AB}$ , where  $\mathbb{1}_B$  denotes the identity in  $\mathcal{P}(\mathcal{H}_B)$ . Isometries from  $\mathcal{H}_A$  to  $\mathcal{H}_B$  are denoted by  $V_{A \rightarrow B}$ .

Completely positive maps from  $\mathcal{L}(\mathcal{H}_A)$  to  $\mathcal{L}(\mathcal{H}_B)$  are called CPMs and trace-preserving CPMs are called TPCPMs. For  $\mathcal{H}_A, \mathcal{H}_B$  with orthonormal bases  $\{|i\rangle_A\}_{i=1}^{|A|}, \{|i\rangle_B\}_{i=1}^{|B|}$  and  $|A| = |B|$ , the canonical identity mapping from  $\mathcal{L}(\mathcal{H}_A)$  to  $\mathcal{L}(\mathcal{H}_B)$  with respect to these bases is denoted by  $\mathcal{I}_{A \rightarrow B}$ , i.e.,  $\mathcal{I}_{A \rightarrow B}(|i\rangle\langle j|_A) = |i\rangle\langle j|_B$ .

For  $\rho \in \mathcal{P}(\mathcal{H})$ ,  $\|\rho\|_\infty$  denotes the operator norm of  $\rho$ , which is equal to the maximum eigenvalue of  $\rho$ . The trace norm of  $\rho \in \mathcal{P}(\mathcal{H})$  is defined as  $\|\rho\|_1 = \text{Tr}(\sqrt{\rho^\dagger \rho})$  and the induced metric on  $\mathcal{S}_{\leq}(\mathcal{H})$  is called trace distance.<sup>3</sup> The fidelity between  $\rho, \sigma \in \mathcal{S}_{\leq}(\mathcal{H})$  is defined as  $F(\rho, \sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1$ .

We will make use of the Choi-Jamiołkowski isomorphism, which relates CPMs to positive operators, and which we denote by  $J$ .

**Lemma 2.1.** [Jam72, Cho75] *The Choi-Jamiołkowski map  $J$  takes maps  $\mathcal{T}^{A \rightarrow B} : \mathcal{L}(\mathcal{H}_A) \rightarrow \mathcal{L}(\mathcal{H}_B)$  to operators  $J(\mathcal{T}^{A \rightarrow B}) \in \mathcal{L}(\mathcal{H}_{A'} \otimes \mathcal{H}_B)$ , where  $\mathcal{H}_{A'} \cong \mathcal{H}_A$ . It is defined as*

$$J(\mathcal{T}^{A \rightarrow B}) = (\mathcal{I}_{A'} \otimes \mathcal{T}^{A \rightarrow B})(|\Phi\rangle\langle\Phi|_{A'A}),$$

where  $|\Phi\rangle_{A'A} = |A|^{-\frac{1}{2}} \sum_i |i\rangle_{A'} \otimes |i\rangle_A$ .<sup>4</sup> The map  $J$  bijectively maps the set of CPMs from  $\mathcal{H}_A$  to  $\mathcal{H}_B$  to the set  $\mathcal{P}(\mathcal{H}_{A'} \otimes \mathcal{H}_B)$ , and its inverse maps any  $\tau_{AB} \in \mathcal{P}(\mathcal{H}_{A'} \otimes \mathcal{H}_B)$  to

$$\mathcal{T}^{A \rightarrow B} : M_A \mapsto |A| \cdot \text{Tr}_A(\tau_{AB} M_A^T),$$

where  $M_A^T$  denotes the transpose of  $M_A$  with respect to the basis  $\{|i\rangle_A\}_{i=1}^{|A|}$ .

### 2.2 Smooth Entropies

The smooth entropy formalism [Ren05, RW04] has been introduced in (classical and quantum) information theory to study general one-shot scenarios, in which nothing needs to be assumed about the structure of the relevant probability distributions or quantum states (e.g., those modeling noise processes in a communication channel). The formalism

<sup>3</sup>The trace distance is often defined with an additional factor  $\frac{1}{2}$ , which we omit here.

<sup>4</sup>The Choi-Jamiołkowski isomorphism is sometimes defined with an additional dimensional factor of  $|A|$ ; we choose not to do this here.

therefore overcomes a limitation of the established theory, where it is usually assumed that the relevant processes can be modeled as asymptotic sequences of *independent and identically distributed (iid)* subprocesses.

In this section we provide the definitions of the underlying entropy measures, called smooth min- and max entropy, and state some of their basic properties. Further properties are summarized in Appendix A. For a more detailed discussion of the smooth entropy formalism we refer to [Ren05, KRS09, TCR09, TCR10, Dat09].

Recall the following standard definitions. The von Neumann entropy of  $\rho \in \mathcal{S}_=(\mathcal{H})$  is defined as<sup>5</sup>  $H(\rho) = -\text{Tr}(\rho \log \rho)$  and the conditional von Neumann entropy of  $A$  given  $B$  for  $\rho_{AB} \in \mathcal{S}_=(\mathcal{H})$  is defined as  $H(A|B)_\rho = H(AB)_\rho - H(B)_\rho$ .

**Definition 2.2.** Let  $\rho_{AB} \in \mathcal{S}_\leq(\mathcal{H}_{AB})$ . The min-entropy of  $A$  conditioned on  $B$  is defined as

$$H_{\min}(A|B)_\rho = \sup_{\sigma_B \in \mathcal{S}_=(\mathcal{H}_B)} \sup\{\lambda \in \mathbb{R} : 2^{-\lambda} \mathbb{1}_A \otimes \sigma_B - \rho_{AB} \geq 0\}.$$

The max-entropy of  $A$  conditioned on  $B$  is defined as

$$H_{\max}(A|B)_\rho = \sup_{\sigma_B \in \mathcal{S}_=(\mathcal{H}_B)} \log F(\rho_{AB}, \mathbb{1}_A \otimes \sigma_B)^2.$$

In the special case where  $B$  is trivial (i.e., one-dimensional), we write  $H_{\min}(A)_\rho$  and  $H_{\max}(A)_\rho$  instead of  $H_{\min}(A|B)_\rho$  and  $H_{\max}(A|B)_\rho$ , respectively. It can be shown that  $H_{\min}(A)_\rho = -\log \|\rho_A\|_\infty$  and  $H_{\max}(A)_\rho = 2 \log \text{Tr} \sqrt{\rho_A}$ .

The smooth min- and max-entropy are defined by extremizing the non-smooth versions over a set of nearby states, where nearby is quantified by the purified distance.

**Definition 2.3.** Let  $\rho, \sigma \in \mathcal{S}_\leq(\mathcal{H})$ . The purified distance between  $\rho$  and  $\sigma$  is defined as

$$P(\rho, \sigma) = \sqrt{1 - \bar{F}(\rho, \sigma)^2},$$

where  $\bar{F}(\rho, \sigma) = F(\rho, \sigma) + \sqrt{(1 - \text{Tr} \rho)(1 - \text{Tr} \sigma)}$  denotes the generalized fidelity.

The purified distance is a distance measure on  $\mathcal{S}_\leq(\mathcal{H})$  [TCR10, Lemma 5]. As its name indicates,  $P(\rho, \sigma)$  corresponds to the minimum trace distance between purifications of  $\rho$  and  $\sigma$ .

Henceforth  $\rho, \sigma \in \mathcal{S}_\leq(\mathcal{H})$  are called  $\varepsilon$ -close if  $P(\rho, \sigma) \leq \varepsilon$  and this is denoted by  $\rho \approx_\varepsilon \sigma$ . We use the purified distance to specify an  $\varepsilon$ -ball around  $\rho \in \mathcal{S}_\leq(\mathcal{H})$ :

$$B^\varepsilon(\rho) = \{\rho' \in \mathcal{S}_\leq(\mathcal{H}) : \rho' \approx_\varepsilon \rho\}.$$

For more about the purified distance we refer to [TCR10].

**Definition 2.4.** Let  $\varepsilon \geq 0$  and  $\rho_{AB} \in \mathcal{S}_\leq(\mathcal{H}_{AB})$ . The  $\varepsilon$ -smooth min-entropy of  $A$  conditioned on  $B$  is defined as

$$H_{\min}^\varepsilon(A|B)_\rho = \sup_{\hat{\rho}_{AB} \in B^\varepsilon(\rho_{AB})} H_{\min}(A|B)_{\hat{\rho}}.$$

The  $\varepsilon$ -smooth max-entropy of  $A$  conditioned on  $B$  is defined as

$$H_{\max}^\varepsilon(A|B)_\rho = \inf_{\hat{\rho}_{AB} \in B^\varepsilon(\rho_{AB})} H_{\max}(A|B)_{\hat{\rho}}.$$

---

<sup>5</sup>All logarithms are taken to base 2.



The min- and max-entropy are dual to each other in the following sense.

**Lemma 2.5.** [TCR10, Lemma 16] Let  $\varepsilon \geq 0$ ,  $\rho_{AB} \in \mathcal{S}_{\leq}(\mathcal{H}_{AB})$  and  $\rho_{ABC} \in \mathcal{S}_{\leq}(\mathcal{H}_{ABC})$  an arbitrary purification of  $\rho_{AB}$ . Then

$$H_{\min}^{\varepsilon}(A|B)_{\rho} = -H_{\max}^{\varepsilon}(A|C)_{\rho}.$$

Smooth entropies satisfy various natural properties analogous to those known for the von Neumann entropy. One of the most important ones is the data processing inequality.

**Lemma 2.6.** [TCR10, Theorem 18] Let  $\varepsilon \geq 0$ ,  $\rho_{AB} \in \mathcal{S}_{\leq}(\mathcal{H}_{AB})$ , and let  $\mathcal{T}_{B \rightarrow C}$  be a TPCPM from  $B$  to  $C$ . Then

$$\begin{aligned} H_{\min}^{\varepsilon}(A|B)_{\rho} &\leq H_{\min}^{\varepsilon}(A|C)_{\mathcal{T}(\rho)} \\ H_{\max}^{\varepsilon}(A|B)_{\rho} &\leq H_{\max}^{\varepsilon}(A|C)_{\mathcal{T}(\rho)}. \end{aligned}$$

Smooth entropies are generalizations of the von Neumann entropy, in the sense that the von Neumann entropy can be retrieved as a special case via the Quantum Asymptotic Equipartition Property (AEP).

**Lemma 2.7.** [Tom12, Corollary 6.6 and 6.7] Let  $0 < \varepsilon < 1$  and  $\rho_{AB} \in \mathcal{S}_{=}(\mathcal{H}_{AB})$ . Then

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{1}{n} H_{\min}^{\varepsilon}(A|B)_{\rho^{\otimes n}} &= H(A|B)_{\rho} \\ \lim_{n \rightarrow \infty} \frac{1}{n} H_{\max}^{\varepsilon}(A|B)_{\rho^{\otimes n}} &= H(A|B)_{\rho}. \end{aligned}$$

For more properties of smooth entropies we refer to the Appendix A and [Ren05, KRS09, TCR09, TCR10, Dat09].

For technical reasons we will also need the following auxiliary quantities.

**Definition 2.8.** Let  $\rho_{AB} \in \mathcal{S}_{\leq}(\mathcal{H}_{AB})$ . The quantum collision entropy of  $A$  given  $B$  is defined as

$$H_2(A|B)_{\rho} = \sup_{\sigma_B \in \mathcal{S}_{=}(\mathcal{H}_B)} -\log \text{Tr} \left[ \left( (\mathbb{1}_A \otimes \sigma_B^{-1/4}) \rho_{AB} (\mathbb{1}_A \otimes \sigma_B^{-1/4}) \right)^2 \right].$$

**Definition 2.9.** Let  $\rho_{AB} \in \mathcal{S}_{\leq}(\mathcal{H}_{AB})$  and  $\sigma_B \in \mathcal{S}_{\leq}(\mathcal{H}_B)$ . We define

$$H_{\max}(A|B)_{\rho|\sigma} := \log F(\rho_{AB}, \mathbb{1}_A \otimes \sigma_B)^2.$$

Note that  $H_{\max}(A|B)_{\rho} = \sup_{\sigma \in \mathcal{S}_{\leq}(\mathcal{H}_B)} H_{\max}(A|B)_{\rho|\sigma}$ .

**Definition 2.10.** Let  $\rho_{AB} \in \mathcal{S}_{\leq}(\mathcal{H}_{AB})$  and  $\sigma_B \in \mathcal{S}_{\leq}(\mathcal{H}_B)$ . We define

$$H_{\min}(A|B)_{\rho|\sigma} := \sup \{ \lambda \in \mathbb{R} : 2^{-\lambda} \mathbb{1}_A \otimes \sigma_B - \rho_{AB} \geq 0 \}.$$

Note that  $H_{\min}(A|B)_{\rho} = \sup_{\sigma \in \mathcal{S}_{\leq}(\mathcal{H}_B)} H_{\min}(A|B)_{\rho|\sigma}$ .

Finally, we note that, since all Hilbert spaces in this paper are assumed to have finite dimension, the infima and suprema in the expressions above can be replaced by minima and maxima, respectively.

### 3 Achievability

In this section, we present and prove a general decoupling theorem (Theorem 3.1), which corresponds to the achievability part of the criterion sketched informally in Section 1. The theorem subsumes and extends most previous results in this direction.

#### 3.1 Statement of the Decoupling Theorem

As explained in the introductory section (see Fig. 1), we consider a mapping from a system  $A$  to a system  $B$ . The mapping consists of a unitary on  $A$ , selected randomly according to the Haar measure over the unitary group on  $\mathcal{H}_A$ , followed by an arbitrary mapping  $\mathcal{T} = \mathcal{T}_{A \rightarrow B}$ . In applications,  $\mathcal{T}$  often consists of a measurement or a partial trace (see Table 2 for examples). The decoupling theorem then tells us how well the output,  $B$ , of the mapping  $\mathcal{T}$  is decoupled (on average over the choices of the unitary) from a reference system  $E$ .

**Theorem 3.1** (Decoupling theorem). *Let  $\varepsilon > 0$ ,  $\rho_{AE} \in \mathcal{S}_=(\mathcal{H}_{AE})$ , and  $\mathcal{T}_{A \rightarrow B}$  a CPM with Choi-Jamiołkowski representation  $\tau_{AB} = J(\mathcal{T})$  such that  $\text{Tr}(\tau_{AB}) \leq 1$ . Then*

$$\int_{\mathbb{U}(A)} \|\mathcal{T}(U\rho_{AE}U^\dagger) - \tau_B \otimes \rho_E\|_1 dU \leq 2^{-\frac{1}{2}H_{\min}^\varepsilon(A|E)_\rho - \frac{1}{2}H_{\min}^\varepsilon(A|B)_\tau} + 12\varepsilon, \quad (1)$$

where  $\int \cdot dU$  denotes the integral over the Haar measure over the full unitary group on  $\mathcal{H}_A$ .

The theorem thus provides a bound on the quality of decoupling that only depends on two entropic quantities,  $H_{\min}^\varepsilon(A|E)_\rho$  and  $H_{\min}^\varepsilon(A|B)_\tau$ . The first is a measure for the correlations between  $A$  and  $E$  that are present in the initial state,  $\rho_{AE}$ . The second quantifies properties of the mapping  $\mathcal{T}$ , which is characterized by the bipartite state  $\tau_{AB}$  obtained via the Choi-Jamiołkowski isomorphism  $J$ . Hence, in order to minimize the right hand side of (1), no channel ends up being better suited for some types of states than for others or vice-versa. Furthermore, as discussed in Section 4, the bound in (1) is essentially optimal in many cases of interest. We also note that, using Markov's inequality, the expectation value over the unitaries  $U$  can be turned into a bound that holds for *most* unitaries. That is, for any  $\mu > 0$ ,

$$\|\mathcal{T}(U\rho_{AE}U^\dagger) - \tau_B \otimes \rho_E\|_1 \leq \frac{1}{\mu} 2^{-\frac{1}{2}H_{\min}^\varepsilon(A|E)_\rho - \frac{1}{2}H_{\min}^\varepsilon(A|B)_\tau} + 12\frac{\varepsilon}{\mu}$$

holds with probability at least  $1 - \mu$  (for  $U$  chosen according to the Haar measure).

Our first step in proving Theorem 3.1 is to prove a version involving non-smooth min-entropies (Theorem 3.2). Then, in a second step, we show that smoothing preserves the essence of the theorem. Note that Theorem 3.2 may be of interest in cases where no smoothing is required since it is slightly more general: it applies to any completely positive  $\mathcal{T}$ , not only trace-non-increasing ones.

**Theorem 3.2** (Non-smooth decoupling theorem). *Let  $\rho_{AE} \in \mathcal{S}_{\leq}(\mathcal{H}_{AE})$  and  $\mathcal{T}_{A \rightarrow B}$  a CPM with Choi-Jamiołkowski representation  $\tau_{AB} = J(\mathcal{T})$ . Then*

$$\int_{\mathbb{U}(A)} \|\mathcal{T}(U\rho_{AE}U^\dagger) - \tau_B \otimes \rho_E\|_1 dU \leq 2^{-\frac{1}{2}H_2(A|E)_\rho - \frac{1}{2}H_2(A|B)_\tau},$$

where  $\int \cdot dU$  denotes the integral over the Haar measure over unitaries  $U$  acting on  $A$ .



### 3.2 Technical Ingredients to the Proof

The proof is based on a few technical lemmas, which we state and prove in the following, and which may be of independent interest. We note that they partly generalize techniques developed in the context of privacy amplification [RK05, Ren05, TRSS10] as well as earlier work on decoupling (see, e.g., [HOW07]).

**Lemma 3.3** (Swap trick). *Let  $M, N \in \mathcal{L}(\mathcal{H}_A)$ . Then  $\text{Tr}[(M \otimes N)F] = \text{Tr}[MN]$ , where  $F$  swaps the two copies of the  $A$  subsystem.*

*Proof.* Write  $M$  and  $N$  in the standard basis for  $\mathcal{H}_A$ :  $M = \sum_{ij} m_{ij} |i\rangle\langle j|$  and  $N = \sum_{kl} n_{kl} |k\rangle\langle l|$ . Then

$$\begin{aligned} \text{Tr}[(M \otimes N)F] &= \text{Tr} \left[ \left( \sum_{ijkl} m_{ij} n_{kl} |i\rangle\langle j| \otimes |k\rangle\langle l| \right) F \right] = \text{Tr} \left[ \sum_{ijkl} m_{ij} n_{kl} |i\rangle\langle l| \otimes |k\rangle\langle j| \right] \\ &= \sum_{ij} m_{ij} n_{ji} = \text{Tr}[MN]. \end{aligned}$$

□

The second lemma involves averaging over Haar distributed unitaries. While it would take us too far afield to formally introduce the Haar measure, it can simply be thought of as the uniform probability distribution over the set of all unitaries on a Hilbert space. The following then tells us the expected value of  $U^{\otimes 2} M (U^\dagger)^{\otimes 2}$  with  $M \in \mathcal{L}(\mathcal{H}_A^{\otimes 2})$  when  $U$  is selected “uniformly at random”.

**Lemma 3.4.** *Let  $M \in \mathcal{L}(\mathcal{H}_A^{\otimes 2})$ . Then*

$$\mathbb{E}(M) := \int_{\mathbb{U}(A)} U^{\otimes 2} M (U^\dagger)^{\otimes 2} dU = \alpha \mathbb{1}_{AA'} + \beta F_A,$$

where  $F_A$  swaps the two copies of the  $A$  subsystem,  $\alpha$  and  $\beta$  are such that  $\text{Tr}[M] = \alpha|A|^2 + \beta|A|$  and  $\text{Tr}[MF] = \alpha|A| + \beta|A|^2$ , and  $dU$  is the normalized Haar measure on  $\mathbb{U}(A)$ .

*Proof.* This follows directly from a standard result in Schur-Weyl duality, e.g., Proposition 2.2 in [CS06]. The latter states that  $\mathbb{E} : \mathcal{L}(\mathcal{H}_A^{\otimes 2}) \rightarrow \mathcal{L}(\mathcal{H}_A^{\otimes 2})$  is an orthogonal projection onto  $\text{span}\{\mathbb{1}, F\}$  under the inner product  $\langle A, B \rangle = \text{Tr}[A^\dagger B]$ . Hence,  $\mathbb{E}(M)$  can be written as  $\alpha \mathbb{1}_{AA'} + \beta F_A$  as claimed, and the conditions  $\text{Tr}[\mathbb{1}\mathbb{E}(M)] = \text{Tr}[M]$  and  $\text{Tr}[F\mathbb{E}(M)] = \text{Tr}[FM]$  must be fulfilled, and these lead to the two conditions on  $\alpha$  and  $\beta$ . □

The following bounds the ratio of the purity of a bipartite state and the purity of the reduced state on one subsystem:

**Lemma 3.5.** *Let  $\xi_{AB} \in \mathcal{P}(\mathcal{H}_{AB})$ . Then*

$$\frac{1}{|A|} \leq \frac{\text{Tr}[\xi_{AB}^2]}{\text{Tr}[\xi_B^2]} \leq |A|.$$

*Proof.* Letting  $A'$  be a system isomorphic to  $A$ , we first prove the left-hand side

$$\begin{aligned}
\text{Tr} [\xi_B^2] &= \text{Tr} [\text{Tr}_A [\xi_{AB}]^2] \\
&= \text{Tr} [\text{Tr}_A [\xi_{AB}] \text{Tr}_{A'} [\xi_{A'B}]] \\
&= \text{Tr} [\xi_{AB} (\text{Tr}_{A'} [\xi_{A'B}] \otimes \mathbb{1}_A)] \\
&= \text{Tr} [(\xi_{AB} \otimes \mathbb{1}_{A'}) (\xi_{A'B} \otimes \mathbb{1}_A)] \\
&\leq \sqrt{\text{Tr} [(\xi_{AB} \otimes \mathbb{1}_{A'})^2] \text{Tr} [(\xi_{A'B} \otimes \mathbb{1}_A)^2]} \\
&= \text{Tr} [\xi_{AB}^2 \otimes \mathbb{1}_{A'}] \\
&= |A| \text{Tr} [\xi_{AB}^2] ,
\end{aligned}$$

where the inequality is due to an application of Cauchy-Schwarz. The right-hand side follows from the fact that  $\xi_{AB} \leq |A| \cdot \mathbb{1}_A \otimes \xi_B$ . This can in turn be seen from the fact that  $|A| \cdot \mathbb{1}_A \otimes \xi_B = \sum_{i=1}^{|A|^2} U_A^i \xi_{AB} (U_A^i)^\dagger$ , where the  $U_A^i$ 's are Weyl operators with  $U_A^1 = \mathbb{1}_A$ .  $\square$

In the main proof, we will need to bound the trace distance between two states. The following lemma will allow us to do this:

**Lemma 3.6.** *Let  $M \in \mathcal{L}(\mathcal{H}_A)$  and  $\sigma \in \mathcal{P}(\mathcal{H}_A)$ . Then*

$$\|M\|_1 \leq \sqrt{\text{Tr}[\sigma] \text{Tr}[\sigma^{-1/4} M \sigma^{-1/2} M^\dagger \sigma^{-1/4}]} .$$

*In particular, if  $M$  is Hermitian then*

$$\|M\|_1 \leq \sqrt{\text{Tr}[\sigma] \text{Tr}[(\sigma^{-1/4} M \sigma^{-1/4})^2]} .$$

This is a slight generalization of Lemma 5.1.3 in [Ren05]; we give a different proof here for completeness.

*Proof.*

$$\begin{aligned}
\|M\|_1 &= \max_U |\text{Tr}[UM]| \\
&= \max_U \left| \text{Tr}[(\sigma^{1/4} U \sigma^{1/4})(\sigma^{-1/4} M \sigma^{-1/4})] \right| \\
&\leq \max_U \sqrt{\text{Tr}[(\sigma^{1/4} U \sigma^{1/4})(\sigma^{1/4} U^\dagger \sigma^{1/4})] \text{Tr}[\sigma^{-1/4} M \sigma^{-1/2} M^\dagger \sigma^{-1/4}]} \\
&= \sqrt{\max_U \text{Tr}[\sigma^{1/2} U \sigma^{1/2} U^\dagger] \text{Tr}[\sigma^{-1/4} M \sigma^{-1/2} M^\dagger \sigma^{-1/4}]} \\
&= \sqrt{\text{Tr}[\sigma] \text{Tr}[\sigma^{-1/4} M \sigma^{-1/2} M^\dagger \sigma^{-1/4}]} ,
\end{aligned}$$

where the inequality results from an application of Cauchy-Schwarz, and the maximizations are over all unitaries on  $A$ . The last equality follows from

$$\begin{aligned}
\max_U \text{Tr}[\sigma^{1/2} U \sigma^{1/2} U^\dagger] &\leq \max_U \sqrt{\text{Tr}[\sigma] \text{Tr}[U \sigma^{1/2} U^\dagger U \sigma^{1/2} U^\dagger]} \\
&= \text{Tr}[\sigma] \\
&\leq \max_U \text{Tr}[\sigma^{1/2} U \sigma^{1/2} U^\dagger] .
\end{aligned}$$

$\square$

### 3.3 Proof of the Non-Smooth Decoupling Theorem (Theorem 3.2)

Throughout the proof, we will denote with a prime the “twin” subsystems used when we take tensor copies of operators, and  $F_S$  denotes a swap between  $S$  and  $S'$ .

We first use Lemma 3.6; for  $\sigma_B \in \mathcal{S}_=(\mathcal{H}_B)$  and  $\zeta_E \in \mathcal{S}_=(\mathcal{H}_E)$  we get

$$\begin{aligned} & \|\mathcal{T}(U\rho_{AE}U^\dagger) - \tau_B \otimes \rho_E\|_1 \\ & \leq \sqrt{\text{Tr} \left[ ((\sigma_B \otimes \zeta_E)^{-1/4} (\mathcal{T}(U\rho_{AE}U^\dagger) - \tau_B \otimes \rho_E) (\sigma_B \otimes \zeta_E)^{-1/4})^2 \right]}. \end{aligned}$$

Now define the CPM  $\tilde{\mathcal{T}}_{A \rightarrow B}(\cdot) = \sigma_B^{-1/4} \mathcal{T}_{A \rightarrow B}(\cdot) \sigma_B^{-1/4}$  and the states  $\tilde{\tau}_{A'B} = J(\tilde{\mathcal{T}})$  and  $\tilde{\rho}_{AE} = \zeta_E^{-1/4} \rho_{AE} \zeta_E^{-1/4}$ . We then rewrite the above as

$$\|\mathcal{T}(U\rho_{AE}U^\dagger) - \tau_B \otimes \rho_E\|_1 \leq \sqrt{\text{Tr} \left[ \left( \tilde{\mathcal{T}}(U\tilde{\rho}_{AE}U^\dagger) - \tilde{\tau}_B \otimes \tilde{\rho}_E \right)^2 \right]}.$$

Using Jensen's inequality we obtain

$$\int \|\mathcal{T}(U\rho_{AE}U^\dagger) - \tau_B \otimes \rho_E\|_1 dU \leq \sqrt{\int \text{Tr} \left[ \left( \tilde{\mathcal{T}}(U\tilde{\rho}_{AE}U^\dagger) - \tilde{\tau}_B \otimes \tilde{\rho}_E \right)^2 \right] dU}. \quad (2)$$

We now simplify the integral

$$\begin{aligned} & \int \text{Tr} \left[ \left( \tilde{\mathcal{T}}(U\tilde{\rho}_{AE}U^\dagger) - \tilde{\tau}_B \otimes \tilde{\rho}_E \right)^2 \right] dU \\ &= \int \text{Tr} \left[ \left( \tilde{\mathcal{T}}(U\tilde{\rho}_{AE}U^\dagger) \right)^2 \right] dU - 2 \int \text{Tr} \left[ \tilde{\mathcal{T}}(U\tilde{\rho}_{AE}U^\dagger) (\tilde{\tau}_B \otimes \tilde{\rho}_E) \right] dU + \text{Tr} \left[ (\tilde{\tau}_B \otimes \tilde{\rho}_E)^2 \right] \\ &= \int \text{Tr} \left[ \left( \tilde{\mathcal{T}}(U\tilde{\rho}_{AE}U^\dagger) \right)^2 \right] dU - 2 \text{Tr} \left[ \tilde{\mathcal{T}} \left( \int U\tilde{\rho}_{AE}U^\dagger dU \right) (\tilde{\tau}_B \otimes \tilde{\rho}_E) \right] + \text{Tr} \left[ (\tilde{\tau}_B \otimes \tilde{\rho}_E)^2 \right] \\ &= \int \text{Tr} \left[ \left( \tilde{\mathcal{T}}(U\tilde{\rho}_{AE}U^\dagger) \right)^2 \right] dU - \text{Tr} [\tilde{\tau}_B^2] \text{Tr} [\tilde{\rho}_E^2]. \end{aligned}$$

We rewrite the first term as follows

$$\begin{aligned} \int \text{Tr} \left[ \left( \tilde{\mathcal{T}}(U\tilde{\rho}_{AE}U^\dagger) \right)^2 \right] dU &= \int \text{Tr} \left[ \left( \tilde{\mathcal{T}}(U\tilde{\rho}_{AE}U^\dagger) \right)^{\otimes 2} F_{BE} \right] dU \\ &= \int \text{Tr} \left[ \left( \tilde{\mathcal{T}}^{\otimes 2} (U^{\otimes 2} \tilde{\rho}_{AE}^{\otimes 2} (U^\dagger)^{\otimes 2}) \right) F_{BE} \right] dU \\ &= \int \text{Tr} \left[ \tilde{\rho}_{AE}^{\otimes 2} \left( \left\{ (U^\dagger)^{\otimes 2} (\tilde{\mathcal{T}}^\dagger)^{\otimes 2} (F_B) U^{\otimes 2} \right\} \otimes F_E \right) \right] dU \\ &= \text{Tr} \left[ \tilde{\rho}_{AE}^{\otimes 2} \left( \int \left\{ (U^\dagger)^{\otimes 2} (\tilde{\mathcal{T}}^\dagger)^{\otimes 2} (F_B) U^{\otimes 2} \right\} dU \otimes F_E \right) \right], \quad (3) \end{aligned}$$

where we have used Lemma 3.3 in the first equality, and the definition of the adjoint of a superoperator in the third equality. We now compute the integral using Lemma 3.4

$$\int (U^\dagger)^{\otimes 2} (\tilde{\mathcal{T}}^\dagger)^{\otimes 2} (F_B) U^{\otimes 2} dU = \alpha \mathbb{1}_{AA'} + \beta F_A$$

where  $\alpha$  and  $\beta$  satisfy the following equations

$$\begin{aligned}\alpha|A|^2 + \beta|A| &= \text{Tr} \left[ (\tilde{\mathcal{T}}^\dagger)^{\otimes 2}(F_B) \right] = \text{Tr} \left[ F_B(\tilde{\mathcal{T}})^{\otimes 2}(\mathbb{1}_{AA'}) \right] = |A|^2 \text{Tr} [F_B \tilde{\tau}_B^{\otimes 2}] \\ &= |A|^2 \text{Tr} [\tilde{\tau}_B^2]\end{aligned}$$

and

$$\begin{aligned}\alpha|A| + \beta|A|^2 &= \text{Tr} \left[ (\tilde{\mathcal{T}}^\dagger)^{\otimes 2}(F_B)F_A \right] = \text{Tr} \left[ F_B \tilde{\mathcal{T}}^{\otimes 2}(F_A) \right] \\ &= |A|^2 \text{Tr} [F_B \text{Tr}_{AA'} [\tilde{\tau}_{AB}^{\otimes 2}(F_A \otimes \mathbb{1}_{BB'})]] \\ &= |A|^2 \text{Tr} [(\mathbb{1}_{AA'} \otimes F_B) \tilde{\tau}_{AB}^{\otimes 2}(F_A \otimes \mathbb{1}_{BB'})] \\ &= |A|^2 \text{Tr} [F_{AB} \tilde{\tau}_{AB}^{\otimes 2}] = |A|^2 \text{Tr} [\tilde{\tau}_{AB}^2].\end{aligned}$$

In the third equality, we have used the fact that  $\tilde{\tau}_{AB}$  is a Choi-Jamiołkowski representation of  $\tilde{\mathcal{T}}$  (Lemma 2.1); the fourth equality is due to the fact that the adjoint of the partial trace is tensoring with the identity.

Solving this system of equations yields

$$\begin{aligned}\alpha &= \text{Tr} [\tilde{\tau}_B^2] \left( \frac{|A|^2 - \frac{|A| \text{Tr} [\tilde{\tau}_{AB}^2]}{\text{Tr} [\tilde{\tau}_B^2]}}{|A|^2 - 1} \right) \\ \beta &= \text{Tr} [\tilde{\tau}_{AB}^2] \left( \frac{|A|^2 - \frac{|A| \text{Tr} [\tilde{\tau}_B^2]}{\text{Tr} [\tilde{\tau}_{AB}^2]}}{|A|^2 - 1} \right).\end{aligned}$$

By applying Lemma 3.5, we can simplify this to  $\alpha \leq \text{Tr} [\tilde{\tau}_B^2]$  and  $\beta \leq \text{Tr} [\tilde{\tau}_{AB}^2]$ . Substituting this into (3) and using Lemma 3.3 twice, and then substituting into (2) yields

$$\int \|\mathcal{T}(U\rho_{AE}U^\dagger) - \tau_B \otimes \rho_E\|_1 dU \leq \sqrt{\text{Tr} [\tilde{\tau}_{AB}^2] \text{Tr} [\tilde{\rho}_{AE}^2]}.$$

Finally we get the theorem by using the definitions of  $\tilde{\tau}_{AB}$ ,  $\tilde{\rho}_{AE}$  and the definition of  $H_2$  (Definition 2.8).

□

### 3.4 Proof of the Main Decoupling Theorem (Theorem 3.1)

We now prove our main result, which is obtained from the non-smooth decoupling theorem (Theorem 3.2) by replacing the collision entropies,  $H_2$ , by smooth min-entropies.

First, note that  $H_2$  is always greater or equal to  $H_{\min}$  (Lemma A.1) and therefore we are allowed to replace the  $H_2$  terms on the right-hand side of the statement of Theorem 3.2 by  $H_{\min}$  terms. Thus we only have to consider the smoothing.

Let  $\hat{\rho}^{AE} \in \mathcal{B}^\varepsilon(\rho_{AE})$  be such that  $H_{\min}^\varepsilon(A|E)_\rho = H_{\min}(A|E)_{\hat{\rho}}$  and  $\hat{\tau}_{AB} \in \mathcal{B}^\varepsilon(\tau_{AB})$  be such that  $H_{\min}^\varepsilon(A|B)_\tau = H_{\min}(A|B)_{\hat{\tau}}$ .

Furthermore write  $\hat{\tau} - \tau = \Delta_+ - \Delta_-$ , where  $\Delta_{\pm} \in \mathcal{P}(\mathcal{H}_{AB})$  have orthogonal support, and likewise,  $\hat{\rho} - \rho = \delta_+ - \delta_-$  with  $\delta_+$  and  $\delta_-$  having orthogonal support. By Lemma B.1 we have  $\|\hat{\tau} - \tau\|_1 \leq 2\varepsilon$  and hence  $\|\Delta_{\pm}\|_1 \leq 2\varepsilon$ .

Moreover define  $\hat{\mathcal{T}}, \mathcal{D}_-$  and  $\mathcal{D}_+$  as the unique superoperators that are such that  $\hat{\tau} = J(\hat{\mathcal{T}})$ ,  $\Delta_- = J(\mathcal{D}_-)$  and  $\Delta_+ = J(\mathcal{D}_+)$  respectively.

Using the non-smooth decoupling theorem (Theorem 3.2) we get

$$\begin{aligned}
& 2^{-\frac{1}{2}H_{\min}^{\varepsilon}(A|B)_{\tau} - \frac{1}{2}H_{\min}^{\varepsilon}(A|E)_{\rho}} \\
& \geq \int_{\mathbb{U}(A)} \left\| \hat{\mathcal{T}}(U\hat{\rho}_{AE}U^{\dagger}) - \hat{\tau}_B \otimes \hat{\rho}_E \right\|_1 dU \\
& \geq \int_{\mathbb{U}(A)} \left\| \hat{\mathcal{T}}(U\hat{\rho}_{AE}U^{\dagger}) - \tau_B \otimes \rho_E \right\|_1 dU - 4\varepsilon. \\
& \geq \int_{\mathbb{U}(A)} \left\| \mathcal{T}(U\rho_{AE}U^{\dagger}) - \tau_B \otimes \rho_E \right\|_1 dU - \int_{\mathbb{U}(A)} \left\| \hat{\mathcal{T}}(U\rho_{AE}U^{\dagger}) - \hat{\mathcal{T}}(U\hat{\rho}_{AE}U^{\dagger}) \right\|_1 dU \\
& \quad - \int_{\mathbb{U}(A)} \left\| \mathcal{T}(U\rho_{AE}U^{\dagger}) - \hat{\mathcal{T}}(U\rho_{AE}U^{\dagger}) \right\|_1 dU - 4\varepsilon.
\end{aligned}$$

We now deal with the second term above

$$\begin{aligned}
\int_{\mathbb{U}(A)} \left\| \hat{\mathcal{T}}(U\rho_{AE}U^{\dagger}) - \hat{\mathcal{T}}(U\hat{\rho}_{AE}U^{\dagger}) \right\|_1 dU &= \int \left\| \hat{\mathcal{T}}(U(\delta_+ - \delta_-)U^{\dagger}) \right\|_1 dU \\
&\leq \int \left\| \hat{\mathcal{T}}(U\delta_+U^{\dagger}) \right\|_1 dU + \int \left\| \hat{\mathcal{T}}(U\delta_-U^{\dagger}) \right\|_1 dU \\
&= \int \text{Tr}[\hat{\mathcal{T}}(U\delta_+U^{\dagger})] dU + \int \text{Tr}[\hat{\mathcal{T}}(U\delta_-U^{\dagger})] dU \\
&= \text{Tr} \left[ \hat{\mathcal{T}} \left( \frac{\mathbb{1}_A}{|A|} \right) \right] (\text{Tr}[\delta_+] + \text{Tr}[\delta_-]) \\
&\leq 4\varepsilon \text{Tr}[\hat{\tau}] \\
&\leq 4\varepsilon.
\end{aligned}$$

We deal with the third term in a similar fashion

$$\begin{aligned}
\int_{\mathbb{U}(A)} \left\| \mathcal{T}(U\rho_{AE}U^{\dagger}) - \hat{\mathcal{T}}(U\rho_{AE}U^{\dagger}) \right\|_1 dU \\
&= \int \|(\mathcal{D}_+ - \mathcal{D}_-)(U\rho_{AE}U^{\dagger})\|_1 dU \\
&\leq \int \|\mathcal{D}_+(U\rho_{AE}U^{\dagger})\|_1 dU + \int \|\mathcal{D}_-(U\rho_{AE}U^{\dagger})\|_1 dU \\
&= \int \text{Tr}[\mathcal{D}_+(U\rho_{AE}U^{\dagger})] dU + \int \text{Tr}[\mathcal{D}_-(U\rho_{AE}U^{\dagger})] dU \\
&= \text{Tr} \left[ \mathcal{D}_+ \left( \frac{\mathbb{1}_A}{|A|} \otimes \rho_E \right) \right] + \text{Tr} \left[ \mathcal{D}_- \left( \frac{\mathbb{1}_A}{|A|} \otimes \rho_E \right) \right] dU \\
&= \text{Tr}[\Delta_+ \otimes \rho_E] + \text{Tr}[\Delta_- \otimes \rho_E] \\
&\leq 4\varepsilon.
\end{aligned}$$

This results in

$$\int_{\mathbb{U}(A)} \left\| \mathcal{T}(U\rho_{AE}U^{\dagger}) - \tau_B \otimes \rho_E \right\|_1 dU \leq 2^{-\frac{1}{2}H_{\min}^{\varepsilon}(A|E)_{\rho} - \frac{1}{2}H_{\min}^{\varepsilon}(A|B)_{\tau}} + 12\varepsilon.$$

□

## 4 Converse

The main purpose of this section is to state and prove a theorem (Theorem 4.1) which implies that the achievability result of the previous section (Theorem 3.1) is essentially optimal for many natural choices of the mapping  $\mathcal{T}$ . More precisely, note that, according to Theorem 3.1, decoupling is achieved whenever the exponent  $H_{\min}^\varepsilon(A|E)_\rho + H_{\min}^\varepsilon(A|B)_\tau$  is sufficiently larger than 0. Our converse now says that this is also a necessary condition (up to additive terms of the order  $\log 1/\varepsilon$ ) if one replaces the min-entropy in the second term,  $H_{\min}^\varepsilon(A|B)_\tau$  (which characterizes the channel), by a max-entropy,  $H_{\max}^\varepsilon(A|B)_\tau$ .

The two terms,  $H_{\min}^\varepsilon(A|B)_\tau$  and  $H_{\max}^\varepsilon(A|B)_\tau$ , coincide for many standard channels used for applications (e.g., for state merging, cf. Section 5). Examples of such channels are given in Table 2. Furthermore, as we shall explain in the discussion section, the two terms also coincide asymptotically for iid channels.

**Theorem 4.1.** *Let  $\rho_{AE} \in \mathcal{S}_=(\mathcal{H}_{AE})$ ,  $\mathcal{T}_{A \rightarrow B}$  a TPCPM, and  $\tau_{AB} = |A| (\sqrt{\rho_A})^\top J(\mathcal{T}) (\sqrt{\rho_A})^\top$ . Suppose that*

$$\|\mathcal{T}(\rho_{AE}) - \mathcal{T}(\rho_A) \otimes \rho_E\|_1 \leq \varepsilon.$$

*Then, for any  $\varepsilon', \varepsilon'' > 0$ ,*

$$H_{\min}^{2\sqrt{6\varepsilon''}+2\varepsilon+2\sqrt{\varepsilon'}+\varepsilon''}(A|E)_\rho + H_{\max}^{\varepsilon''}(A|B)_\tau \geq -\log \frac{1}{\varepsilon'}.$$

Note that in the above,  $\tau_{AB}$  can be produced by taking a purification  $\zeta_{AA'}$  of  $\rho_A$  where the system  $A'$  is a copy of  $A$ , and sending the  $A'$  part through the channel.

*Proof.* Let  $\rho_{AER}$  be a purification of  $\rho_{AE}$  and  $U_{A \rightarrow BB'}^\mathcal{T}$  a Stinespring dilation of  $\mathcal{T}$ . Furthermore, let

$$|\tilde{\sigma}\rangle_{BB'ER} := (U_{A \rightarrow BB'}^\mathcal{T} \otimes \mathbb{1}_{ER})|\rho\rangle_{AER},$$

and  $|\sigma\rangle_{BB'ER}$  be a subnormalized state such that  $H_{\max}(ER|B)_\sigma = H_{\max}^{\varepsilon''}(A|B)_\tau$  with  $P(\sigma, \tilde{\sigma}) \leq \varepsilon''$ , as well as  $|\bar{\sigma}\rangle_{BB'ER}$  such that  $\bar{\sigma}_{BE} = \sigma_B \otimes \sigma_E$ , and  $F(\sigma_{BB'ER}, \bar{\sigma}_{BB'ER}) = F(\sigma_{BE}, \sigma_B \otimes \sigma_E)$  — such a state exists by Uhlmann's theorem, and can be shown to satisfy  $P(\bar{\sigma}, \sigma) \leq \sqrt{6\varepsilon''} + 2\varepsilon$ . The latter bound can be obtained from

$$\begin{aligned} \|\sigma_{BE} - \bar{\sigma}_{BE}\|_1 &\leq \|\sigma_{BE} - \tilde{\sigma}_{BE}\|_1 + \|\tilde{\sigma}_{BE} - \bar{\sigma}_{BE}\|_1 \\ &\leq \|\sigma_{BE} - \tilde{\sigma}_{BE}\|_1 + \|\tilde{\sigma}_{BE} - \tilde{\sigma}_B \otimes \tilde{\sigma}_E\|_1 + \|\tilde{\sigma}_B \otimes \tilde{\sigma}_E - \sigma_B \otimes \sigma_E\|_1 \\ &\leq \varepsilon'' + \varepsilon + \|\tilde{\sigma}_B \otimes \tilde{\sigma}_E - \tilde{\sigma}_B \otimes \sigma_E\|_1 + \|\tilde{\sigma}_B \otimes \sigma_E - \sigma_B \otimes \sigma_E\|_1 \\ &\leq 3\varepsilon'' + \varepsilon, \end{aligned}$$

combined with Lemma B.1. Now, we know from Lemma A.8 that

$$\sigma_{BB'ER} \leq 2^{H_{\max}(ER|B)_{\sigma|\sigma}} Y_{EBR} \otimes \mathbb{1}_{B'},$$

where

$$Y_{BER} := 2^{-\frac{1}{2}H_{\max}(ER|B)_{\sigma|\sigma}} \sigma_B^{-1/2} \sqrt{\sigma_B^{1/2} \sigma_{BER} \sigma_B^{1/2}} \sigma_B^{-1/2}.$$



This implies that

$$\sigma_{BB'ER} \leq \frac{1}{\varepsilon'} \cdot 2^{H_{\max}(ER|B)_{\sigma|\sigma}} \left( (1 - \varepsilon') \sigma_B^{-1/2} \bar{\sigma}_{BER} \sigma_B^{-1/2} + \varepsilon' Y_{BER} \right) \otimes \mathbb{1}_{B'} \quad (4)$$

for any  $\varepsilon' > 0$ . Tracing out the  $R$  system, we get

$$\sigma_{BEB'} \leq \frac{1}{\varepsilon'} \cdot 2^{H_{\max}(ER|B)_{\sigma|\sigma}} \left( (1 - \varepsilon') \mathbb{1}_B \otimes \sigma_E + \varepsilon' Y_{BE} \right) \otimes \mathbb{1}_{B'}.$$

We now define  $G_{BE} := \sqrt{1 - \varepsilon'} \sigma_E^{1/2} ((1 - \varepsilon') \mathbb{1}_B \otimes \sigma_E + \varepsilon' Y_{BE})^{-1/2}$ . Note that  $G$  is a contraction (i.e.  $\|G\|_{\infty} \leq 1$ ):

$$\begin{aligned} GG^{\dagger} &= (1 - \varepsilon') \sigma_E^{1/2} \left( (1 - \varepsilon') \mathbb{1}_B \otimes \sigma_E + \varepsilon' Y_{BE} \right)^{-1} \sigma_E^{1/2} \\ &\leq (1 - \varepsilon') \sigma_E^{1/2} \left( (1 - \varepsilon') \mathbb{1}_B \otimes \sigma_E \right)^{-1} \sigma_E^{1/2} \\ &= \mathbb{1}_{BE}, \end{aligned}$$

where we have used the operator monotonicity of  $f(t) = -1/t$ . At this point, we conjugate both sides of (4) by  $G_{BE}$  to get

$$G_{BE} \sigma_{BEB'} G_{BE}^{\dagger} \leq \frac{1 - \varepsilon'}{\varepsilon'} \cdot 2^{H_{\max}(ER|B)_{\sigma|\sigma}} \sigma_E \otimes \mathbb{1}_{BB'} \quad (5)$$

$$\leq \frac{1}{\varepsilon'} \cdot 2^{H_{\max}(ER|B)_{\sigma|\sigma}} \sigma_E \otimes \mathbb{1}_{BB'}. \quad (6)$$

Let us now define  $|\psi\rangle_{BEB'} := G_{BE} |\sigma\rangle_{BEB'}$ ; note that since  $G$  is a contraction,  $|\psi\rangle$  is subnormalized. Then, we can rewrite (6) as:

$$|\psi\rangle_{BEB'} \leq \frac{1}{\varepsilon'} \cdot 2^{H_{\max}(ER|B)_{\sigma|\sigma}} \sigma_E \otimes \mathbb{1}_{BB'},$$

which implies

$$H_{\min}(BB'|E)_{\psi|\sigma} \geq -H_{\max}(ER|B)_{\sigma|\sigma} - \log(1/\varepsilon').$$

We will now need to show that  $\psi_{BEB'}$  is  $(2\sqrt{6\varepsilon''} + 2\varepsilon + 2\sqrt{\varepsilon'} + \varepsilon'')$ -close to  $\tilde{\sigma}_{BEB'}$ , because this implies the claim

$$H_{\min}^{2\sqrt{6\varepsilon''} + 2\varepsilon + 2\sqrt{\varepsilon'} + \varepsilon''}(A|E)_{\rho} + H_{\max}^{\varepsilon''}(A|B)_{\tau} \geq -\log(1/\varepsilon').$$

To this end, we shall define the following states

$$\begin{aligned} |\psi'\rangle_{BEB'} &:= G_{BE}^{\dagger} |\bar{\sigma}\rangle_{BEB'} \\ |\psi''\rangle_{BEB'} &:= G_{BE} |\bar{\sigma}\rangle_{BEB'} \\ |\tilde{\psi}\rangle_{BEB'} &:= \sqrt{1 - \varepsilon'} G_{BE}^{-1} |\bar{\sigma}\rangle_{BEB'}. \end{aligned}$$

We first show that all these states are (sub)-normalized such that the purified distance between them is well-defined. Since  $G_{BE}$  is a contraction, we immediately get that  $\|\psi'\rangle\| \leq 1$  and  $\|\psi''\rangle\| \leq 1$ . Furthermore,

$$\begin{aligned} \|\tilde{\psi}\rangle\|^2 &= (1 - \varepsilon') \langle \bar{\sigma} | G_{BE}^{-1 \dagger} G_{BE}^{-1} | \bar{\sigma} \rangle \\ &= \langle \bar{\sigma} | \sigma_E^{-1/2} \left( (1 - \varepsilon') \mathbb{1}_B \otimes \sigma_E + \varepsilon' Y_{BE} \right) \sigma_E^{-1/2} | \bar{\sigma} \rangle \\ &= 1 - \varepsilon' + \varepsilon' \langle \bar{\sigma} | \sigma_E^{-1/2} Y_{BE} \sigma_E^{-1/2} | \bar{\sigma} \rangle \\ &= 1 - \varepsilon' + \varepsilon' \text{Tr} \left[ Y_{BE} \sigma_E^{-1/2} \bar{\sigma}_{EB} \sigma_E^{-1/2} \right] \\ &= 1 - \varepsilon' + \varepsilon' \text{Tr} [Y_{BE} \sigma_B] \\ &= 1. \end{aligned}$$

We have  $\langle \tilde{\psi} | \psi' \rangle = \sqrt{1 - \varepsilon'}$ , and

$$\begin{aligned}
\langle \bar{\sigma} | \tilde{\psi} \rangle &= \sqrt{1 - \varepsilon'} \langle \bar{\sigma} | G_{BE}^{-1} | \bar{\sigma} \rangle \\
&= \text{Tr} \left[ (\sigma_B \otimes \sigma_E) \left( (1 - \varepsilon') \mathbb{1}_B \otimes \sigma_E + \varepsilon' Y_{BE} \right)^{1/2} \sigma_E^{-1/2} \right] \\
&= \text{Tr} \left[ (\sigma_B \otimes \sigma_E^{1/2}) \left( (1 - \varepsilon') \mathbb{1}_B \otimes \sigma_E + \varepsilon' Y_{BE} \right)^{1/2} \right] \\
&\geq \text{Tr} \left[ (\sigma_B \otimes \sigma_E^{1/2}) \sqrt{1 - \varepsilon'} (\mathbb{1}_B \otimes \sigma_E^{1/2}) \right] \\
&= \sqrt{1 - \varepsilon'} \text{Tr} [\sigma_B \otimes \sigma_E] \\
&= \sqrt{1 - \varepsilon'} ,
\end{aligned}$$

where the inequality is due to the operator monotonicity of the square-root function. Therefore  $P(\psi', \bar{\sigma}) \leq 2\sqrt{\varepsilon'}$  and furthermore  $P(\psi'', \bar{\sigma}) = P(\psi', \bar{\sigma})$ , since

$$F(\psi'', \bar{\sigma}) = \langle \bar{\sigma} | G_{BE}^\dagger | \bar{\sigma} \rangle = F(\bar{\sigma}, \psi') .$$

Since conjugation by  $G$  is trace-non-increasing, we also have

$$P(\psi'', \psi) \leq P(\sigma, \bar{\sigma}) \leq \sqrt{6\varepsilon'' + 2\varepsilon} .$$

This implies

$$P(\psi, \tilde{\sigma}) \leq P(\psi, \psi'') + P(\psi'', \bar{\sigma}) + P(\bar{\sigma}, \sigma) + P(\sigma, \tilde{\sigma}) \leq \sqrt{6\varepsilon'' + 2\varepsilon} + 2\sqrt{\varepsilon'} + \sqrt{6\varepsilon'' + 2\varepsilon} + \varepsilon'' .$$

□

## 5 One-Shot State Merging

As an example application of the decoupling theorem and its converse we discuss *One-Shot Quantum State Merging*. This is a two-party task: its goal is to transfer the information contained in a quantum system,  $A$ , initially held by one party, Alice, to the other party, Bob. This should be achieved with only limited resources (such as entanglement or communication). It is taken into account that Bob may have access to a quantum system,  $B$ , correlated to  $A$ , which may be used to minimize the use of resources. The term *one-shot* is used to emphasize that the task is considered in the general one-shot scenario. As explained in the discussion section, the asymptotic iid results, where many independent copies of a given state are transferred, can be recovered as a special case.

The notion of quantum state merging has been introduced in [HOW05, HOW07] and a protocol has been proposed that achieves the task in the asymptotic iid scenario. The more general one-shot setup we consider here was first analyzed in [Ber08] and preliminary results appeared in [KRS09].

We start giving a formal definition of quantum state merging [HOW05, HOW07, Ber08]. Let  $\rho_{AB}$  be the joint initial state of Alice and Bob's systems. We can view this state as part of a larger pure state  $\rho_{ABE}$  that includes a reference system  $E$ . In this picture state merging means that Alice can send the  $A$ -part of  $\rho_{ABE}$  to Bob's side without altering the joint state. We consider the particular setting proposed in [HOW05] where classical communication from Alice to Bob is free, but no quantum communication is possible. Furthermore, Alice and Bob have access to a source of entanglement and their goal is to minimize the number of entangled bits consumed during the protocol (or maximize the number of entangled bits that can be generated).

**Definition 5.1** (Quantum State Merging). Let  $\rho_{AB} \in \mathcal{S}_=(\mathcal{H}_{AB})$ , and let  $A_0B_0$  be additional systems. A TPCPM  $\mathcal{E} : AA_0 \otimes BB_0 \rightarrow A_1 \otimes B_1B'B$  is called Quantum State Merging of  $\rho_{AB}$  with error  $\varepsilon \geq 0$ , if it is a local operation and classical forward communication process for the bipartition  $AA_0 \rightarrow A_1$  vs.  $BB_0 \rightarrow B_1B'B$ , and

$$(\mathcal{E} \otimes \mathcal{I}_E)(\Phi_{A_0B_0}^K \otimes \rho_{ABE}) \approx_\varepsilon \Phi_{A_1B_1}^L \otimes \rho_{BB'E} ,$$

where  $\rho_{BB'E} = (\mathcal{I}_{A \rightarrow B'} \otimes \mathcal{I}_{BE})\rho_{ABE}$  for a purification  $\rho_{ABE}$  of  $\rho_{AB}$ , and  $\Phi^K, \Phi^L$  are maximally entangled states on  $A_0B_0, A_1B_1$  of Schmidt-rank  $K$  and  $L$ , respectively. The number

$$l^\varepsilon := \log K - \log L$$

is called entanglement cost.<sup>6</sup>

We are interested in quantifying the minimal entanglement cost for Quantum State Merging of  $\rho_{AB}$  with error  $\varepsilon$ . For this, we use the achievability and converse for decoupling (Theorem 3.1 and Theorem 4.1). These allow us to derive essentially tight (up to additive terms of the order  $\log 1/\varepsilon$ ) bounds on the entanglement cost.

The basic idea underlying our analysis of Quantum State Merging is the observation that the desired situation after the protocol execution is necessarily such that Alice's system is decoupled from the reference. Furthermore, it follows from Uhlmann's theorem [Uhl76] that this decoupling is also sufficient.

**Theorem 5.2** (Achievability for Quantum State Merging). *The minimal entanglement cost for Quantum State Merging of  $\rho_{AB} \in \mathcal{S}_=(\mathcal{H}_{AB})$  with error  $\varepsilon > 0$  is upper bounded by*

$$l^\varepsilon \leq H_{\max}^{\varepsilon^2/13}(A|B)_\rho + 4 \log(1/\varepsilon) + 2 \log 13 .$$

*Proof.* Let  $\rho_{ABE}$  be a purification of  $\rho_{AB}$ . The intuition is as follows. In the first step of the protocol, Alice decouples her part from the reference (employing Theorem 3.1), where she chooses a rank- $L$  projective measurement as the TPCPM, and she sends the measurement result to Bob. For all measurement outcomes the post-measurement state on Alice's side is then approximately given by  $\frac{\mathbb{1}_{A_1}}{|A_1|} \otimes \rho_E$  and Bob holds a purification of this. But  $\frac{\mathbb{1}_{A_1}}{|A_1|} \otimes \rho_E$  is the reduced state of  $\Phi_{A_1B_1}^L \otimes \rho_{BB'E}$  as well and since all purifications are equal up to local isometries, there exists an isometry on Bob's side that transform the state into  $\Phi_{A_1B_1}^L \otimes \rho_{BB'E}$  (by Uhlmann's theorem [Uhl76]); this is then the second step of the protocol.

More formally, choose  $K$  and  $L$  such that

$$\log K - \log L = H_{\max}^{\varepsilon^2/13}(A|B)_\rho + 4 \log(1/\varepsilon) + 2 \log 13 , \quad (7)$$

which is the entanglement cost of the protocol.<sup>7</sup>

<sup>6</sup>In the original references [HOW05, HOW07] quantum state merging was defined slightly differently, namely as a local operation and classical two-way communication process. However, their protocol for the achievability only uses classical forward communication.

<sup>7</sup>Since we need  $K, L \in \mathbb{N}$ , we can not choose  $\log K - \log L$  exactly equal to  $H_{\max}^{\varepsilon^2/13}(A|B)_\rho + 4 \log(1/\varepsilon) + 2 \log 13$  in general. Rather, we need to choose  $K, L \in \mathbb{N}$  such  $\log K - \log L$  is minimal but still greater or equal then  $H_{\max}^{\varepsilon^2/13}(A|B)_\rho + 4 \log(1/\varepsilon) + 2 \log 13$ .

Choose  $N$  fixed orthogonal subspaces of dimension  $L$  on  $AA_0$ ,<sup>8</sup> denote the projectors on these subspaces followed by a fixed unitary mapping it to  $A_1$  by  $P_{A_0A \rightarrow A_1}^x$  and define the isometry

$$W_{A_0A \rightarrow A_1X_AX_B} := \sum_x P_{A_0A \rightarrow A_1}^x \otimes |x\rangle_{X_A} \otimes |x\rangle_{X_B}. \quad (8)$$

Denote by  $U_{A_0A}$  a unitary selected randomly according to the Haar measure over the unitary group on  $\mathcal{H}_{A_0A}$  and write

$$\begin{aligned} \theta_{A_0B_0ABE} &:= \Phi_{A_0B_0}^K \otimes \rho_{ABE} \\ \sigma_{A_0B_0ABE} &:= U_{A_0A} \theta_{A_0B_0ABE} U_{A_0A}^\dagger. \end{aligned}$$

Now the first step of the protocol is to apply this unitary followed by the isometry (8), and to send the  $X_B$  system to Bob. In order to take into account that the channel is classical, we keep a copy  $X_A$  at Alice's side.

By the decoupling theorem (Theorem 3.1) we get for

$$\sigma_{A_1X_AX_BB_0BE} = (W_{A_0A \rightarrow A_1X_AX_B}) \sigma_{A_0B_0ABE} (W_{A_0A \rightarrow A_1X_AX_B})^\dagger.$$

that

$$\|\sigma_{A_1X_AE} - \tau_{A_1X_A} \otimes \rho_E\|_1 \leq 2^{-1/2(H_{\min}^{\varepsilon^2/13}(A_0A|E)_\theta + H_{\min}^{\varepsilon^2/13}(A'_0A'|A_1X_A)_\tau)} + \frac{12}{13} \cdot \varepsilon^2, \quad (9)$$

where  $A'_0A'$  is a copy of  $A_0A$ , and

$$|\tau\rangle_{A'_0A'A_1X_AX_B} := W_{A_0A \rightarrow A_1X_AX_B} |\Phi\rangle_{A'_0A'A_0A}$$

with

$$|\Phi\rangle_{A'_0A'A_0A} := \frac{1}{K \cdot |A|} \sum_i |i\rangle_{A'_0A'} \otimes |i\rangle_{A_0A}.$$

We can simplify this using the superadditivity of smooth min-entropy (Lemma A.2) and the duality between min- and max-entropy (Lemma 2.5)

$$H_{\min}^{\varepsilon^2/13}(A_0A|E)_\theta \geq H_{\min}^{\varepsilon^2/13}(A|E)_\rho + \log K = -H_{\max}^{\varepsilon^2/13}(A|B)_\rho + \log K. \quad (10)$$

Furthermore, because  $\tau_{A'_0A'A_1X_A}$  is classical on  $X_A$ , we can use a lemma about the min-entropy of classical-quantum states (Lemma A.5) and get

$$\begin{aligned} H_{\min}^{\varepsilon^2/13}(A'_0A'|A_1X_A)_\tau &\geq H_{\min}(A'_0A'|A_1X_A)_\tau = -\log\left(\sum_x p_x \cdot 2^{-H_{\min}(A'_0A'|A_1)_{\tau^x}}\right) \\ &\geq \min_x H_{\min}(A'_0A'|A_1)_{\tau^x}, \end{aligned}$$

where

$$\begin{aligned} \tau_{A'_0A'A_1}^x &:= \frac{1}{\sqrt{p_x}} (\mathbb{1}_{A'_0A'} \otimes P_{A_0A \rightarrow A_1}^x) |\Phi\rangle_{A'_0A'A_0A} \\ p_x &:= |(\mathbb{1}_{A'_0A'} \otimes P_{A_0A \rightarrow A_1}^x) |\Phi\rangle_{A'_0A'A_0A}|^2. \end{aligned}$$

---

<sup>8</sup>For simplicity assume that  $K \cdot |A|$  is divisible by  $L$ . In general one has to choose  $N - 1$  fixed orthogonal subspaces of dimension  $L$  and one of dimension  $L' = K \cdot |A| - (N - 1) \cdot L < L$ . The proof remains the same, although some coefficients change.

But since  $P_{A_0A \rightarrow A_1}^x$  is a rank  $L$  projector, we can use a dimension lower bound of the min-entropy (Lemma A.3) to conclude that for all  $x$

$$H_{\min}(A'_0 A' | A_1)_{\tau^x} \geq -\log L.$$

This together with (7), (9) and (10) implies

$$\begin{aligned} \left\| \sigma_{A_1 X_A E} - \frac{\mathbb{1}_{A_1}}{|A_1|} \otimes \tau_{X_A} \otimes \rho_E \right\|_1 &= \left\| \sigma_{A_1 X_A E} - \tau_{A_1 X_A} \otimes \rho_E \right\|_1 \\ &\leq 2^{-1/2(\log K - \log L - H_{\max}^{\varepsilon^{2/13}}(A|B)_\rho)} + \frac{12}{13} \cdot \varepsilon^2 \\ &= 2^{-1/2(4 \log(1/\varepsilon) + 2 \log 13)} + \frac{12}{13} \cdot \varepsilon^2 = \varepsilon^2, \end{aligned}$$

and hence  $F(\sigma_{A_1 X_A E}, \frac{\mathbb{1}_{A_1}}{|A_1|} \otimes \tau_{X_A} \otimes \rho_E) \geq 1 - \frac{1}{2}\varepsilon^2$  (by Lemma B.1).

In the second step of the protocol, Bob decodes the system to the state  $\rho_{BB'E} \otimes \Phi_{A_1 B_1}$ . A suitable decoder can be shown to exist using Uhlmann's theorem [Uhl76]. There exists an isometry  $V_{BB_0 X_B \rightarrow BB' B_1 X_B}$  such that for

$$\begin{aligned} \eta_{A_1 X_A X_B BB' B_1 E} &:= (V_{BB_0 X_B \rightarrow BB' B_1 X_B}) \sigma_{A_1 X_A X_B BB_0 E} (V_{BB_0 X_B \rightarrow BB' B_1 X_B})^\dagger \\ F(\sigma_{A_1 X_A E}, \frac{\mathbb{1}_{A_1}}{|A_1|} \otimes \tau_{X_A} \otimes \rho_E) &= F(\eta_{A_1 X_A X_B BB' B_1 E}, \tau_{X_A X_B} \otimes \Phi_{A_1 B_1}^L \otimes \rho_{BB'E}), \end{aligned}$$

and with that

$$F(\eta_{A_1 X_A X_B BB' B_1 E}, \tau_{X_A X_B} \otimes \Phi_{A_1 B_1}^L \otimes \rho_{BB'E}) \geq 1 - \frac{1}{2}\varepsilon^2. \quad (11)$$

Expressing this in the purified distance (with Lemma B.1) and discarding  $X_A X_B$ , we obtain a  $\varepsilon$ -error Quantum State Merging protocol for  $\rho_{ABE}$ .  $\square$

**Theorem 5.3** (Converse for Quantum State Merging). *The minimal entanglement cost for Quantum State Merging of  $\rho_{AB} \in \mathcal{S}_=(\mathcal{H}_{AB})$  with error  $\varepsilon > 0$  is lower bounded by*

$$l^\varepsilon \geq H_{\max}^{4\sqrt{2\varepsilon}+3\varepsilon}(A|B)_\rho - 2 \log \frac{1}{\varepsilon}.$$

*Proof.* We start with noting that any  $\varepsilon$ -error Quantum State Merging protocol for  $\rho_{AB}$  can be assumed to have the following form: applying local operations at Alice's side, then sending a classical register from Alice to Bob, and finally applying local operations at Bob's side. For a purified state  $\rho_{ABE}$ , the protocol produces a state  $\varepsilon$ -close to  $\Phi_{A_1 B_1}^L \otimes \rho_{BB'E}$ .

As can be seen from the definition, it is a necessary step for any Quantum State Merging protocol to decouple Alice's part from the reference. The idea of the proof is to use the converse for decoupling (Theorem 4.1). This then results in the desired converse for Quantum State Merging.

More precisely, a general  $\varepsilon$ -error Quantum State Merging protocol for  $\rho_{ABE}$  has the following form. At first some TPCPM

$$\mathcal{T}_{A_0 A \rightarrow A_1 X_B}(\cdot) = \sum_x M_{A_0 A \rightarrow A_1}^x(\cdot) \otimes |x\rangle\langle x|_{X_B}$$

is applied to the input state  $\Phi_{A_0 B_0}^K \otimes \rho_{ABE}$ . By the Stinespring dilation [Sti55] we can think of this TPCPM as an isometry

$$W_{A_0 A \rightarrow A_1 A_G X_B X_A} = \sum_x M_{A_0 A \rightarrow A_1 A_G}^x \otimes |x\rangle_{X_A} \otimes |x\rangle_{X_B}, \quad (12)$$

where the  $M_{A_0 A \rightarrow A_1 A_G}^x$  are partial isometries and  $A_G, X_A$  are additional ‘garbage’ registers on Alice’s side that will be discarded in the end. The isometry  $W$  results in the state

$$|\gamma\rangle_{A_1 A_G X_A X_B B B_0 E} := \sum_x |\gamma^x\rangle_{A_1 A_G B B_0 E} \otimes |x\rangle_{X_A} \otimes |x\rangle_{X_B},$$

with

$$|\gamma^x\rangle_{A_1 A_G B B_0 E} := M_{A_0 A \rightarrow A_1 A_G}^x (|\Phi^K\rangle_{A_0 B_0} \otimes |\rho\rangle_{ABE}).$$

The next step of the protocol is then to send the classical register  $X_B$  to Bob.

Now let us analyze how the state  $\gamma_{A_1 A_G X_A E}$  has to look like. By the definition of Quantum State Merging (Definition 5.1) the state at the end of the protocol has to be  $\varepsilon$ -close to  $\Phi_{A_1 B_1}^L \otimes \rho_{BB'E}$ . This implies that Alice’s part  $A_1$  has to be decoupled from the reference. But because the state  $\Phi_{A_1 B_1}^L \otimes \rho_{BB'E}$  is pure this also implies that all additional registers, that we might have at the end of the protocol, have to be decoupled as well. Thus we need

$$\gamma_{A_1 A_G X_A E} \approx_\varepsilon \frac{\mathbb{1}_{A_1}}{|A_1|} \otimes \gamma_{A_G X_A} \otimes \rho_E, \quad (13)$$

and in trace distance (using Lemma B.1) this reads

$$\left\| \gamma_{A_1 A_G X_A E} - \frac{\mathbb{1}_{A_1}}{|A_1|} \otimes \gamma_{A_G X_A} \otimes \rho_E \right\|_1 \leq 2\varepsilon. \quad (14)$$

Using the converse for decoupling (Theorem 4.1) for the isometry  $W_{A_0 A \rightarrow A_1 A_G X_B X_A}$  in (12) followed by the partial trace over  $X_B$ , we get that the decoupling condition (14) implies for any  $\varepsilon', \varepsilon'' > 0$  that

$$H_{\min}^{2\sqrt{6\varepsilon''}+2\varepsilon+2\sqrt{\varepsilon'}+\varepsilon''}(A_0 A|E)_\rho + H_{\max}^{\varepsilon''}(A'_0 A'|A_1 A_G X_A)_\tau \geq -\log \frac{1}{\varepsilon'},$$

where

$$\tau_{A'_0 A' A_1 A_G X_A} := \text{tr}_{X_B} \left[ (\mathbb{1}_{A'_0 A'} \otimes W_{A_0 A \rightarrow A_1 A_G X_B X_A}) \zeta_{A'_0 A' A_0 A} (\mathbb{1}_{A'_0 A'} \otimes W_{A_0 A \rightarrow A_1 A_G X_B X_A}^\dagger) \right]$$

for  $\zeta_{A'_0 A' A_0 A}$  a purification of  $\frac{\mathbb{1}_{A_0}}{|A_0|} \otimes \rho_A$  with  $A'_0 A'$  a copy of  $A_0 A$ . As a next step we simplify this in order to bring the converse into the desired form.

Choosing  $\varepsilon' = \varepsilon^2$  and  $\varepsilon'' = \varepsilon$ , using a dimension upper bound for smooth min-entropy (Lemma A.4), and the duality of min- and max-entropy (Lemma 2.5) we obtain

$$\log K + H_{\max}^\varepsilon(A'_0 A'|A_1 A_G X_A)_\tau \geq H_{\max}^{4\sqrt{2\varepsilon}+3\varepsilon}(A|B)_\rho - 2 \log \frac{1}{\varepsilon}.$$



By the decoupling criterion in purified distance (Equation (13)), the state  $\tau_{A'_0 A' A_1 A_G X_A}$  has to be  $\varepsilon$ -close to a state

$$\xi_{A'_0 A' A_1 A_G X_A} = \sum_x q_x \xi_{A'_0 A' A_1 A_G}^x \otimes |x\rangle\langle x|_{X_A} ,$$

where  $q_x$  is some probability distribution and  $\xi_{A'_0 A' A_1 A_G}^x$  pure with  $\xi_{A_1 A_G}^x = \frac{\mathbb{1}_{A_1}}{|A_1|} \otimes \xi_{A_G}^x$  for all  $x$ . Hence

$$H_{\max}^\varepsilon(A'_0 A' | A_1 A_G X_A)_\tau \leq H_{\max}(A'_0 A' | A_1 A_G X_A)_\xi$$

and by a lemma about the max-entropy of classical quantum states (Lemma A.6)

$$H_{\max}(A'_0 A' | A_1 A_G X_A)_\xi = \log \left( \sum_x q_x \cdot 2^{H_{\max}(A'_0 A' | A_1 A_G)_{\xi^x}} \right) .$$

Using the duality of min- and max-entropy (Lemma 2.5) and a polar decomposition of  $\xi_{A'_0 A' A_1 A_G}^x$ , we get

$$\begin{aligned} H_{\max}(A'_0 A' | A_1 A_G)_{\xi^x} &= -H_{\min}(A'_0 A')_{\xi^x} = -H_{\min}(A_1 A_G)_{\xi^x} \\ &= -H_{\min}(A_1)_{\frac{\mathbb{1}}{|A_1|}} - H_{\min}(A_G)_{\xi^x} \leq -H_{\min}(A_1)_{\frac{\mathbb{1}}{|A_1|}} = -\log L . \end{aligned}$$

Hence the converse becomes

$$\log K - \log L \geq H_{\max}^{4\sqrt{2\varepsilon}+3\varepsilon}(A|B)_\rho - 2 \log \frac{1}{\varepsilon} .$$

□

## 6 Discussion

The main contribution of this work is a decoupling theorem, i.e., a sufficient (Theorem 3.1) and necessary (Theorem 4.1) criterion for decoupling in terms of smooth entropies. The fact that the criterion is nearly optimal for various choices of the decoupling map  $\mathcal{T}$  suggests that use of smooth entropies is natural in this context.

A crucial property of our decoupling theorem is that it is valid in a *one-shot scenario*, where the decoupling map  $\mathcal{T}$  may only be applied once (or, by replacing  $\mathcal{T}$  by  $\mathcal{T}^{\otimes k}$ , any finite number of times). This contrasts with (and is strictly more general than) the *iid scenario*<sup>9</sup> usually considered in information theory, where results are stated and proved asymptotically under the assumption that the underlying processes (such as channel uses) are repeated many times independently. The generalization to the one-shot scenario is particularly relevant in the context of applications in physics (e.g., the study of black hole radiation as considered in [HP07, BP07, BZ09] or the analysis of thermodynamic systems [dRAR<sup>+</sup>11]), where the channel  $\mathcal{T}$  is supposed to model the evolution of a single system.

We note that asymptotic iid statements can be easily retrieved from the general one-shot results using the Quantum Asymptotic Equipartition Property (AEP) for smooth

<sup>9</sup>The abbreviation *iid* stands for *independent and identically distributed*.

entropies [Ren05, TCR09] (see Lemma 2.7). For this, the decoupling map  $\mathcal{T}$  as well as the initial state  $\rho_{AE}$  need to be replaced by many identical copies of themselves, i.e.,  $\mathcal{T}^{\otimes n}$  and  $\rho_{AB}^{\otimes n}$ . The achievability bound of Theorem 3.1, i.e., the condition that is sufficient for decoupling, then turns into the criterion

$$H(A|E)_\rho + H(A|B)_\tau \geq 0, \quad (15)$$

where  $H$  denotes the (conditional) von Neumann entropy. Analogously, the converse, i.e., the condition which is necessary for decoupling, turns into

$$H(A|E)_\rho + H(A|B)_\tau \leq 0, \quad (16)$$

In other words, in the iid scenario, the achievability bound (15) and the converse bound (16), taken together, imply an exact characterization of decoupling.

The decoupling theorem, in its general form stated in Section 3, has various applications. As illustrated in Section 5, these are often possible because of a duality between independence and maximum entanglement: given a pure state  $\rho_{BER}$  such that  $\rho_B$  is maximally mixed, the property that the subsystem  $B$  is independent of  $E$  and the property that  $B$  is fully entangled with  $R$  are equivalent.

Information-theoretic applications other than state merging (cf. Section 5) have been investigated in [Dup09]. One of them is *channel coding*. Here, Alice wants to use a noisy quantum channel  $\mathcal{N}^{A \rightarrow B}$  to send qubits to Bob with fidelity at least  $1 - \varepsilon$ . The idea is that decoding is possible whenever a purification of the qubits Alice is sending is decoupled from the channel environment. One can therefore get a coding theorem directly from Theorem 3.1 by setting  $\mathcal{T}$  to be the complementary channel of  $\mathcal{N}$  (i.e. consider a Stinespring dilation  $U_{\mathcal{N}}^{A \rightarrow BE}$  of  $\mathcal{N}$ , and set  $\mathcal{T}^{A \rightarrow E}(\cdot) := \text{Tr}_B[U \cdot U^\dagger]$ ). Unassisted channel coding [Llo97, Sho02, Dev05] can be obtained by choosing the input state  $\rho_{AR} = \Phi_{AR}$  (where  $\Phi_{AR}$  is a maximally entangled state between  $A$  and  $R$ ). Similarly, entanglement-assisted channel coding [BSST02] corresponds to the input choice  $\rho_{ABR} = \Phi_{ARR} \otimes \Phi_{ABB}$  (where  $\mathcal{H}_A = \mathcal{H}_{AR} \otimes \mathcal{H}_{AB}$ , with  $A_R$  containing the state to be transmitted and  $A_B$  the initial entanglement that Alice shares with Bob). Other choices of  $\rho_{ABR}$  correspond to other scenarios.

Another application where decoupling can be employed as a building block for constructing protocols is the simulation of noisy quantum channels using perfect classical channels together with pre-shared entanglement. The claim that this is possible using only a classical communication rate equal to the capacity of the channel to be simulated, is known as the *Fully Quantum Reverse Shannon Theorem* [BSST02, BDH<sup>+</sup>09]. In [BCR11], a proof of this theorem using the decoupling technique has been proposed.

## Acknowledgments

We thank Andreas Winter for insightful discussions and for his valuable contributions to [Ber08], which served as a starting point for this work. We also thank Patrick Hayden for enlightening discussions, as well as Oleg Szehr for fixing a bug regarding smoothing in the proof of Theorem 3.1, among other useful comments. We acknowledge support from the Swiss National Science Foundation (grants No. 200021-119868 and 200020-135048) as well as from the European Research Council (grant No. 258932). FD was supported by Canada's NSERC Postdoctoral Fellowship Program. MB is supported by the

Swiss National Science Foundation (grant PP00P2-128455) and the German Science Foundation (grants CH 843/1-1 and CH 843/2-1). JW was funded by the U.K. EPSRC grant EP/E04297X/1 and the Canada-France NSERC-ANR project FREQUENCY. Parts of this work were done while JW was at the University of Bristol.

## References

- [ADHW09] Anura Abeyesinghe, Igor Devetak, Patrick Hayden, and Andreas Winter. The mother of all protocols: Restructuring quantum information’s family tree. *Proceedings of the Royal Society A*, 465:2537, 2009. arXiv:quant-ph/0606225v1.
- [BBCM95] Charles H. Bennett, Gilles Brassard, Claude Crépeau, and Ueli Maurer. Generalized privacy amplification. *IEEE Transactions on Information Theory*, 41:1915, 1995.
- [BCR11] Mario Berta, Matthias Christandl, and Renato Renner. The quantum reverse Shannon theorem based on one-shot information theory. *Communications in Mathematical Physics*, 306:579, 2011. arXiv:0912.3805v3.
- [BDH<sup>+</sup>09] Charles H. Bennett, Igor Devetak, Aram W. Harrow, Peter W. Shor, and Andreas Winter. Quantum reverse Shannon theorem. arXiv:0912.5537v2, 2009.
- [Ber08] Mario Berta. Single-shot quantum state merging. Diploma Thesis, ETH Zürich, 2008. arXiv:0912.4495v1.
- [BP07] Samuel L. Braunstein and Arun K. Pati. Quantum information cannot be completely hidden in correlations: Implications for the black-hole information paradox. *Physical Review Letters*, 98:080502, 2007. arXiv:gr-qc/0603046v.
- [BRW07] Mario Berta, Renato Renner, and Andreas Winter. Tightness of decoupling by projective measurements. Unpublished manuscript; the technical proof appeared as part of [Ber08], 2007.
- [BSST02] Charles H. Bennett, Peter W. Shor, John A. Smolin, and Ashish V. Thapliyal. Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem. *IEEE Transactions on Information Theory*, 48:2637, 2002. arXiv:quant-ph/0106052v2.
- [Bus09] Francesco Buscemi. Private quantum decoupling and secure disposal of information. *New Journal of Physics*, 11:123002, 2009. arXiv:0901.4506v5.
- [BZ09] Samuel L. Braunstein and Karol Zyczkowski. Entangled black holes as ciphers of hidden information. arXiv:0907.1190v2, 2009.
- [Cho75] Man-Duen Choi. Completely positive linear maps on complex matrices. *Linear algebra and its applications*, 10:285, 1975.
- [CS06] Benoît Collins and Piotr Śniady. Integration with respect to the Haar measure on unitary, orthogonal and symplectic group. *Communications in Mathematical Physics*, 264:773, 2006. arXiv:math-ph/0402073v1.

- [Dat09] Nilanjana Datta. Min- and max- relative entropies and a new entanglement monotone. *IEEE Transactions on Information Theory*, 55:2816, 2009. arXiv:0803.2770v3.
- [Dev05] Igor Devetak. The private classical capacity and quantum capacity of a quantum channel. *IEEE Transactions on Information Theory*, 51:44, 2005. arXiv:quant-ph/0304127v6.
- [dRAR<sup>+</sup>11] L dia del Rio, Johan  berg, Renato Renner, Oscar Dahlsten, and Vlatko Vedral. The thermodynamic meaning of negative entropy. *Nature*, 474:61, 2011. arXiv:1009.1630v2.
- [DRRV09] Oscar Dahlsten, Renato Renner, Elisabeth Rieper, and Vlatko Vedral. Inadequacy of von Neumann entropy for characterizing extractable work. *New Journal of Physics*, 13:053015, 2009. arXiv:0908.0424v1.
- [Dup09] Fr d ric Dupuis. *The decoupling approach to quantum information theory*. PhD thesis, Universit  de Montr al, 2009. arXiv:1004.1641v1.
- [GPW05] Berry Groisman, Sandu Popescu, and Andreas Winter. Quantum, classical, and total amount of correlations in quantum state. *Physical Review A*, 72:032317, 2005. arXiv:quant-ph/0410091v2.
- [HHWY08] Patrick Hayden, Micha  Horodecki, Andreas Winter, and Jon Yard. A decoupling approach to the quantum capacity. *Open Systems and Information Dynamics*, 15:7, 2008. arXiv:quant-ph/0702005v1.
- [HOW05] Micha  Horodecki, Jonathan Oppenheim, and Andreas Winter. Partial quantum information. *Nature*, 436:673, 2005. arXiv:quant-ph/0505062v1.
- [HOW07] Micha  Horodecki, Jonathan Oppenheim, and Andreas Winter. Quantum state merging and negative information. *Communications in Mathematical Physics*, 269:107, 2007. arXiv:quant-ph/0512247v1.
- [HP07] Patrick Hayden and John Preskill. Black holes as mirrors: quantum information in random subsystems. *Journal of High Energy Physics*, 07:120, 2007. arXiv:0708.4025v2.
- [Jam72] Andrzej Jamio kowski. Linear transformations which preserve trace and positive semidefiniteness of operators. *Reports on Mathematical Physics*, 3:275, 1972.
- [KRS09] Robert K nig, Renato Renner, and Christian Schaffner. The operational meaning of min- and max-entropy. *IEEE Transactions on Information Theory*, 55:4337, 2009. arXiv:0807.1338v1.
- [Llo97] Seth Lloyd. Capacity of the noisy quantum channel. *Physical Review A*, 55:1613, 1997. arXiv:quant-ph/9604015v25.
- [LPSW09] Noah Linden, Sandu Popescu, Anthony J. Short, and Andreas Winter. Quantum mechanical evolution towards thermal equilibrium. *Physical Review E*, 79:061103, 2009. arXiv:0812.2385v1.
- [Par89a] M. Hossein Partovi. Irreversibility, reduction, and entropy increase in quantum measurements. *Physics Letters A*, 137:445, 1989.

- [Par89b] M. Hossein Partovi. Quantum thermodynamics. *Physics Letters A*, 137:440, 1989.
- [Ren05] Renato Renner. *Security of quantum key distribution*. PhD thesis, ETH Zurich, 2005. arXiv:quant-ph/0512258v2.
- [Ren09] Renato Renner. Optimal decoupling. *Proceedings of the International Congress on Mathematical Physics*, page 541, 2009.
- [RK05] Renato Renner and Robert König. Universally composable privacy amplification against quantum adversaries. In *Second Theory of Cryptography Conference TCC*, volume 3378 of *Lecture Notes in Computer Science*, page 407. Springer, 2005. arXiv:quant-ph/0403133v2.
- [RW04] Renato Renner and Stefan Wolf. Smooth Rényi entropy and applications. In *Proceedings International Symposium on Information Theory*, page 233, 2004.
- [Sho02] Peter Shor. The quantum channel capacity and coherent information. *Lecture notes, MSRI workshop on quantum computation*, 2002. <http://www.msri.org/publications/ln/msri/2002/quantumcrypto/shor/1/>.
- [Sti55] W. Forrest Stinespring. Positive function on  $C^*$ -algebras. *Proceedings American Mathematical Society*, 6:211, 1955.
- [TCR09] Marco Tomamichel, Roger Colbeck, and Renato Renner. A fully quantum asymptotic equipartition property. *IEEE Transactions on Information Theory*, 55:5840, 2009. arXiv:0811.1221v3.
- [TCR10] Marco Tomamichel, Roger Colbeck, and Renato Renner. Duality between smooth min- and max-entropies. *IEEE Transactions on Information Theory*, 56:4674, 2010. arXiv:0907.5238v2.
- [Tom12] Marco Tomamichel. *A framework for non-asymptotic quantum information theory*. PhD thesis, ETH Zurich, 2012. arXiv:1203.2142v1.
- [TRSS10] Marco Tomamichel, Renato Renner, Christian Schaffner, and Adam Smith. Leftover hashing against quantum side information. In *Information Theory Proceedings (ISIT), 2010 IEEE International Symposium on*, page 2703, 2010. arXiv:1002.2436v1.
- [Uhl76] Armin Uhlmann. The ‘transition probability’ in the state space of a  $*$ -algebra. *Reports on Mathematical Physics*, 9:273, 1976.
- [Wat08] John Watrous. *Theory of Quantum Information—Lecture notes from Fall 2008*. 2008. [www.cs.uwaterloo.ca/~watrous/quant-info/](http://www.cs.uwaterloo.ca/~watrous/quant-info/).
- [WR09] Jürg Wullschleger and Renato Renner. A generalized decoupling theorem for partial traces and projective measurements. unpublished manuscript; the technical proof appeared in the appendix of [BCR11], 2009.

## A Properties of Smooth Entropies

**Lemma A.1.** *Let  $\rho_{AB} \in \mathcal{S}_{\leq}(\mathcal{H}_{AB})$ . Then,  $H_2(A|B)_\rho \geq H_{\min}(A|B)_\rho$ .*

*Proof.* Let  $\sigma_B \in \mathcal{S}_=(\mathcal{H}_B)$  be such that  $\rho_{AB} \leq 2^{-H_{\min}(A|B)_\rho} \mathbb{1}_A \otimes \sigma_B$ . We then obtain

$$\begin{aligned} 2^{-H_2(A|B)_\rho} &= \min_{\omega_B} \text{Tr} \left[ (\mathbb{1}_A \otimes \omega_B)^{-1/2} \rho_{AB} (\mathbb{1}_A \otimes \omega_B)^{-1/2} \rho_{AB} \right] \\ &\leq \text{Tr} \left[ (\mathbb{1}_A \otimes \sigma_B)^{-1/2} \rho_{AB} (\mathbb{1}_A \otimes \sigma_B)^{-1/2} \rho_{AB} \right] \\ &\leq 2^{-H_{\min}(A|B)_\rho} \text{Tr} [\mathbb{1}_{AB} \rho_{AB}] \\ &\leq 2^{-H_{\min}(A|B)_\rho} . \end{aligned}$$

□

**Lemma A.2** (Superadditivity of smooth min-entropy). *Let  $\varepsilon, \varepsilon' \geq 0$ ,  $\rho_{AB} \in \mathcal{S}_=(\mathcal{H}_{AB})$  and  $\rho'_{A'B'} \in \mathcal{S}_=(\mathcal{H}_{A'B'})$ . Then*

$$H_{\min}^{\varepsilon+\varepsilon'}(AA'|BB')_{\rho \otimes \rho'} \geq H_{\min}^\varepsilon(A|B)_\rho + H_{\min}^{\varepsilon'}(A'|B')_{\rho'} .$$

*Proof.* Let  $\bar{\rho}_{AB} \in \mathcal{B}^\varepsilon(\rho_{AB})$  and  $\bar{\rho}'_{A'B'} \in \mathcal{B}^{\varepsilon'}(\rho'_{A'B'})$  such that  $H_{\min}^\varepsilon(A|B)_\rho = H_{\min}(A|B)_{\bar{\rho}}$  and  $H_{\min}^{\varepsilon'}(A'|B')_{\rho'} = H_{\min}(A'|B')_{\bar{\rho}'}$ .

By the triangle inequality for the purified distance [TCR10, Lemma 5] we have  $\bar{\rho}_{AB} \otimes \bar{\rho}'_{A'B'} \in \mathcal{B}^{\varepsilon+\varepsilon'}(\rho_{AB} \otimes \rho'_{A'B'})$ . Using the additivity of min-entropy [KRS09] we conclude

$$\begin{aligned} H_{\min}^{\varepsilon+\varepsilon'}(AA'|BB')_{\rho \otimes \rho'} &\geq H_{\min}(AA'|BB')_{\bar{\rho} \otimes \bar{\rho}'} = H_{\min}(A|B)_{\bar{\rho}} + H_{\min}(A'|B')_{\bar{\rho}'} \\ &= H_{\min}^\varepsilon(A|B)_\rho + H_{\min}^{\varepsilon'}(A'|B')_{\rho'} . \end{aligned}$$

□

**Lemma A.3.** [TCR10, Lemma 20] *Let  $\rho_{AB} \in \mathcal{S}_=(\mathcal{H}_{AB})$ . Then  $H_{\min}(A|B)_\rho \geq -\log |B|$ .*

**Lemma A.4.** *Let  $\varepsilon \geq 0$  and  $\rho_{ABC} \in \mathcal{S}_=(\mathcal{H}_{ABC})$ . Then*

$$H_{\min}^\varepsilon(AB|C)_\rho \leq H_{\min}^\varepsilon(A|C)_\rho + \log |B| .$$

*Proof.* Let  $\bar{\rho}_{ABC} \in \mathcal{B}^\varepsilon(\rho_{ABC})$ ,  $\sigma_C \in \mathcal{S}_=(\mathcal{H}_C)$  and  $\lambda \in \mathbb{R}$  such that

$$H_{\min}^\varepsilon(AB|C)_\rho = H_{\min}(AB|C)_{\bar{\rho}} = -\log \lambda ,$$

that is,  $\lambda$  is minimal such that  $\lambda \cdot \mathbb{1}_{AB} \otimes \sigma_C - \bar{\rho}_{ABC} \geq 0$ . By taking the partial trace over  $B$  we get  $\lambda \cdot |B| \cdot \mathbb{1}_A \otimes \sigma_C - \bar{\rho}_{AC} \geq 0$ . Furthermore we have by the monotonicity of the purified distance [TCR10, Lemma 7] that  $\bar{\rho}_{AC} \in \mathcal{B}^\varepsilon(\rho_{AC})$  and hence

$$H_{\min}^\varepsilon(A|C)_\rho \geq H_{\min}(A|C)_{\bar{\rho}} \geq -\log \mu ,$$

where  $\mu \in \mathbb{R}$  is minimal such that  $\mu \cdot \mathbb{1}_A \otimes \sigma_C - \bar{\rho}_{AC} \geq 0$ . Thus  $\lambda \cdot |B| \geq \mu$  and therefore

$$H_{\min}^\varepsilon(AB|C)_\rho \leq H_{\min}^\varepsilon(A|C)_\rho + \log |B| .$$

□



**Lemma A.5.** Let  $\rho_{ABX} \in \mathcal{S}_=(\mathcal{H}_{ABX})$  with  $\rho_{ABX} = \sum_x p_x \rho_{AB}^x \otimes |x\rangle\langle x|_X$  and  $\rho_{AB}^x \in \mathcal{S}_=(\mathcal{H}_{AB})$  for all  $x$ . Then

$$H_{\min}(A|BX)_\rho = -\log\left(\sum_x p_x \cdot 2^{-H_{\min}(A|B)_{\rho^x}}\right). \quad (17)$$

*Proof.* By the operational interpretation of the min-entropy as the maximal achievable singlet fraction [KRS09, Theorem 2] we have

$$H_{\min}(A|BX)_\rho = -\log(|A| \cdot \max_{\mathcal{F}_{BX \rightarrow A'}} F^2((\mathcal{I}_A \otimes \mathcal{F}_{BX \rightarrow A'}) (\rho_{ABX}), |\Phi\rangle\langle\Phi|_{AA'})),$$

where the maximum is taken over all TPCPMs  $\mathcal{F}_{BX \rightarrow A'}$ ,  $|\Phi\rangle_{AA'} = |A|^{-1/2} \sum_i |x\rangle_A \otimes |x\rangle_{A'}$ , and  $\mathcal{H}_{A'} \cong \mathcal{H}_A$ . Writing out the min-entropy terms on the right hand side of (17) in the same manner we obtain

$$H_{\min}(A|B)_{\rho^x} = -\log(|A| \cdot \max_{\mathcal{F}_{B \rightarrow A'}^x} F^2((\mathcal{I}_A \otimes \mathcal{F}_{B \rightarrow A'}^x) (\rho_{AB}^x), |\Phi\rangle\langle\Phi|_{AA'})).$$

The claim of the lemma is therefore equivalent to

$$\begin{aligned} \max_{\mathcal{F}_{BX \rightarrow A'}} F^2((\mathcal{I}_A \otimes \mathcal{F}_{BX \rightarrow A'}) (\rho_{ABX}), |\Phi\rangle\langle\Phi|_{AA'}) \\ = \sum_x p_x \max_{\mathcal{F}_{B \rightarrow A'}^x} F^2((\mathcal{I}_A \otimes \mathcal{F}_{B \rightarrow A'}^x) (\rho_{AB}^x), |\Phi\rangle\langle\Phi|_{AA'}). \end{aligned}$$

Now, because the state  $\rho_{ABX}$  is classical on  $X$ , the maximization on the left hand side can without loss of generality be restricted to TPCPMs that first measure on  $X$  in the basis  $\{|x\rangle\}$  and then do some TPCPM  $\mathcal{F}_{B \rightarrow A'}^x$  conditioned on the measurement outcome  $x$ . By the linearity of the square of the fidelity when one argument is pure, the claim then follows.  $\square$

**Lemma A.6.** Let  $\rho_{ABX} \in \mathcal{S}_=(\mathcal{H}_{ABX})$  with  $\rho_{ABX} = \sum_x p_x \rho_{AB}^x \otimes |x\rangle\langle x|_X$  and  $\rho_{AB}^x \in \mathcal{S}_=(\mathcal{H}_{AB})$  for all  $x$ . Then

$$H_{\max}(A|BX)_\rho = \log\left(\sum_x p_x \cdot 2^{H_{\max}(A|B)_{\rho^x}}\right). \quad (18)$$

*Proof.* Let  $\rho_{ABCX'X'}$  be a purification of  $\rho_{ABX}$ . Then we have by the duality of conditional min- and max-entropy (Lemma 2.5) and a lemma about the conditional min-entropy of classical quantum state (Lemma A.5) that

$$H_{\max}(A|BX)_\rho = -H_{\min}(A|CX')_\rho = \log\left(\sum_x p_x \cdot 2^{-H_{\min}(A|C)_{\rho^x}}\right) = \log\left(\sum_x p_x \cdot 2^{H_{\max}(A|B)_{\rho^x}}\right).$$

$\square$

**Lemma A.7** (Chain rule for smooth min-entropy). Let  $\varepsilon > 0$ ,  $\varepsilon', \varepsilon'' \geq 0$  and  $\rho_{ABC} \in \mathcal{S}_=(\mathcal{H}_{ABC})$ . Then

$$H_{\min}^{\varepsilon+2\varepsilon'+\varepsilon''}(AB|C)_\rho \geq H_{\min}^{\varepsilon'}(A|BC)_\rho + H_{\min}^{\varepsilon''}(B|C)_\rho - \log \frac{2}{\varepsilon^2}$$

*Proof.* Let  $\rho'_{ABC} \in \mathcal{B}^{\varepsilon'}(\rho_{ABC})$  such that  $H_{\min}^{\varepsilon'}(A|BC)_{\rho} = H_{\min}(A|BC)_{\rho'}$  and let  $\rho'_{ABCE}$  be a purification of  $\rho'_{ABC}$ . Furthermore let  $\rho''_{BC} \in \mathcal{B}^{\varepsilon''}(\rho_{BC})$ ,  $\sigma_C \in \mathcal{S}_=(\mathcal{H}_{BC})$  and  $\lambda \in \mathbb{R}$  such that  $H_{\min}^{\varepsilon''}(B|C)_{\rho} = H_{\min}(B|C)_{\rho''} = -\log \lambda$ , that is,  $\lambda$  is minimal such that

$$\lambda \cdot \mathbb{1}_B \otimes \sigma_C - \rho''_{BC} \geq 0. \quad (19)$$

By [TRSS10, Lemma 21] there exists a projector  $P_{AE}$  such that

$$\bar{\rho}'_{ABCE} := (P_{AE} \otimes \mathbb{1}_{BC})\rho'_{ABCE}(P_{AE} \otimes \mathbb{1}_{BC}) \in \mathcal{B}^{\varepsilon}(\rho'_{ABCE}),$$

and

$$2^{-H_{\min}^{\varepsilon'}(A|BC)_{\rho} + \log \frac{2}{\varepsilon^2}} \cdot \mathbb{1}_A \otimes \rho'_{BC} - \bar{\rho}'_{ABC} \geq 0. \quad (20)$$

Now let  $T_{BC}$  be defined as in Lemma B.2 with  $\rho''_{BC} = T_{BC}\rho'_{BC}T_{BC}^{\dagger}$  and consider the state

$$\bar{\rho}''_{ABCE} := (\mathbb{1}_{AE} \otimes T_{BC})\bar{\rho}'_{ABCE}(\mathbb{1}_{AE} \otimes T_{BC}^{\dagger}) = (P_{AE} \otimes T_{BC})\rho'_{ABCE}(P_{AE} \otimes T_{BC}^{\dagger}).$$

Applying  $T_{BC}$  to (20) we obtain

$$2^{-H_{\min}^{\varepsilon'}(A|BC)_{\rho} + \log \frac{2}{\varepsilon^2}} \cdot \mathbb{1}_A \otimes \rho''_{BC} - \bar{\rho}''_{ABC} \geq 0.$$

Together with (19) this yields

$$2^{-H_{\min}^{\varepsilon'}(A|BC)_{\rho} + \log \frac{2}{\varepsilon^2} - H_{\min}^{\varepsilon''}(B|C)_{\rho}} \cdot \mathbb{1}_{AB} \otimes \sigma_C - \bar{\rho}''_{ABC} \geq 0.$$

This implies

$$H_{\min}(AB|C)_{\bar{\rho}''} \geq H_{\min}^{\varepsilon'}(A|BC)_{\rho} + H_{\min}^{\varepsilon''}(B|C)_{\rho} - \log \frac{2}{\varepsilon^2}. \quad (21)$$

But by the monotonicity of the purified distance [TCR10, Lemma 7] and the definition of  $T_{BC}$  we have

$$\begin{aligned} P(\bar{\rho}''_{ABC}, \bar{\rho}'_{ABC}) &\leq P((P_{AE} \otimes T_{BC})\rho'_{ABCE}(P_{AE} \otimes T_{BC}^{\dagger}), (P_{AE} \otimes \mathbb{1}_{BC})\rho'_{ABCE}(P_{AE} \otimes \mathbb{1}_{BC})) \\ &\leq P((\mathbb{1}_{AE} \otimes T_{BC})\rho'_{ABCE}(\mathbb{1}_{AE} \otimes T_{BC}^{\dagger}), \rho'_{ABCE}) = P(\rho''_{BC}, \rho'_{BC}), \end{aligned}$$

and hence

$$P(\bar{\rho}''_{ABC}, \bar{\rho}'_{ABC}) \leq P(\rho''_{BC}, \rho_{BC}) + P(\rho_{BC}, \rho'_{BC}) \leq \varepsilon'' + \varepsilon'.$$

Finally we obtain

$$\begin{aligned} P(\bar{\rho}''_{ABC}, \rho_{ABC}) &\leq P(\bar{\rho}''_{ABC}, \bar{\rho}'_{ABC}) + P(\bar{\rho}'_{ABC}, \rho'_{ABC}) + P(\rho'_{ABC}, \rho_{ABC}) \\ &\leq \varepsilon'' + \varepsilon' + \varepsilon + \varepsilon' = \varepsilon + 2\varepsilon' + \varepsilon', \end{aligned}$$

and thus together with (21) that

$$H_{\min}^{\varepsilon + 2\varepsilon' + \varepsilon'}(AB|C)_{\rho} \geq H_{\min}^{\varepsilon'}(A|BC)_{\rho} + H_{\min}^{\varepsilon''}(B|C)_{\rho} - \log \frac{2}{\varepsilon^2}.$$

□

**Lemma A.8.** Let  $\rho_{ABC} \in \mathcal{S}_{\leq}(\mathcal{H}_{ABC})$  be a pure state. Then, for  $\sigma_B \in \mathcal{S}_{=}(H_B)$  with full rank, we have that

$$\rho_{ABC} \leq Z_{AB} \otimes \mathbb{1}_C,$$

where  $Z_{AB} = 2^{\frac{1}{2}H_{\max}(A|B)_{\rho|\sigma}} \sigma_B^{-1/2} \sqrt{\sigma_B^{1/2} \rho_{AB} \sigma_B^{1/2}} \sigma_B^{-1/2}$ . Furthermore,  $Z_{AB}$  has the property that  $\text{Tr}[Z_{AB} \sigma_B] = 2^{H_{\max}(A|B)_{\rho|\sigma}}$ .

*Proof.* Consider the following semidefinite program (for an introduction to semidefinite programs presented in this manner, see for instance [Wat08]):

<u>Primal</u>	<u>Dual</u>
maximize: $\text{Tr}[\rho_{ABC} X_{ABC}]$	minimize: $\text{Tr}[(\mathbb{1}_A \otimes \sigma_B) Z_{AB}]$
subject to: $\text{Tr}_C[X_{ABC}] = \mathbb{1}_A \otimes \sigma_B$	subject to: $\rho_{ABC} \leq Z_{AB} \otimes \mathbb{1}_C$ .
$X_{ABC} \geq 0$ .	

It is clear that the optimal value of the primal problem is  $2^{H_{\max}(A|B)_{\rho|\sigma}}$  from Definition 2.9 and Uhlmann's theorem. One can also easily show that strong duality holds (i.e. that the optimal value of the dual problem is equal to that of the primal problem): one simply needs to show that there exists a  $Z_{AB}$  such that  $Z_{AB} \otimes \mathbb{1}_C > \rho_{ABC}$ , which holds for  $Z_{AB} = 2\mathbb{1}_{AB}$ .

Now, we need to show that the optimal  $Z_{AB}$  for this problem has the form given in the lemma statement. First, note that by Uhlmann's theorem, there must exist an optimal  $X_{ABC}$  which has rank 1, assuming we consider the system  $C$  to be large enough. Let  $X_{ABC} = |\varphi\rangle\langle\varphi|_{ABC}$  and let  $\rho_{ABC} = |\rho\rangle\langle\rho|_{ABC}$ , and consider the complementary slackness condition for  $X$  and  $Z$  to be optimal:  $\rho_{ABC} X_{ABC} = (Z_{AB} \otimes \mathbb{1}_C) X_{ABC}$ . We can rewrite this as

$$\langle\rho|\varphi\rangle|\rho\rangle\langle\varphi| = (Z_{AB} \otimes \mathbb{1}_C)|\varphi\rangle\langle\varphi|$$

and therefore

$$\langle\rho|\varphi\rangle|\rho\rangle = (Z_{AB} \otimes \mathbb{1}_C)|\varphi\rangle,$$

and

$$F(\rho, \varphi)^2 |\rho\rangle\langle\rho| = (Z_{AB} \otimes \mathbb{1}_C) |\varphi\rangle\langle\varphi| (Z_{AB} \otimes \mathbb{1}_C).$$

Tracing out  $C$  and using the fact that  $F(\rho, \varphi)^2 = 2^{H_{\max}(A|B)_{\rho|\sigma}}$ , we get

$$2^{H_{\max}(A|B)_{\rho|\sigma}} \rho_{AB} = Z_{AB} (\mathbb{1}_A \otimes \sigma_B) Z_{AB}.$$

Now, conjugating both sides by  $\sigma_B^{1/2}$  and taking square roots on both sides, we get that

$$2^{\frac{1}{2}H_{\max}(A|B)_{\rho|\sigma}} \sqrt{\sigma_B^{1/2} \rho_{AB} \sigma_B^{1/2}} = \sigma_B^{1/2} Z_{AB} \sigma_B^{1/2}.$$

If  $\sigma_B$  has full rank, we get the expression for  $Z_{AB}$  by conjugating both sides by  $\sigma_B^{-1/2}$ . Finally, the fact that  $\text{Tr}[Z_{AB} \sigma_B] = 2^{H_{\max}(A|B)_{\rho|\sigma}}$  can simply be computed from the expression for  $Z$ .

□

## B Technical Lemmas

**Lemma B.1** (Lemma 6 in [TCR10]). *Let  $\rho, \sigma \in \mathcal{S}_{\leq}(\mathcal{H})$ . Then,*

$$\begin{aligned} \bar{D}(\rho, \sigma) &\leq P(\rho, \sigma) \leq \sqrt{2\bar{D}(\rho, \sigma)} \leq \sqrt{2\|\rho - \sigma\|_1} \\ \frac{1}{2}P(\rho, \sigma)^2 &\leq \bar{D}(\rho, \sigma) \leq P(\rho, \sigma). \end{aligned}$$

where  $\bar{D}(\rho, \sigma) := \frac{1}{2}\|\rho - \sigma\|_1 + \frac{1}{2}|\text{Tr}[\rho] - \text{Tr}[\sigma]|$ .

**Lemma B.2.** *Let  $\rho_{AB} \in \mathcal{S}_{\leq}(\mathcal{H}_{AB})$  and  $\sigma_A \in \mathcal{S}_{\leq}(\mathcal{H}_A)$ . Then there exists  $T_A \in \mathcal{L}(\mathcal{H}_A)$  with*

$$\sigma_{AB} := (T_A \otimes \mathbb{1}_B)\rho_{AB}(T_A^\dagger \otimes \mathbb{1}_B) \in \mathcal{S}_{\leq}(\mathcal{H}_{AB})$$

*an extension of  $\sigma_A$  such that  $P(\rho_{AB}, \sigma_{AB}) = P(\rho_A, \sigma_A)$ .*

*Proof.* Define  $X_A := \sigma_A^{\frac{1}{2}}\rho_A^{\frac{1}{2}}$  and polar decompose  $X_A = V_A \cdot (X_A^\dagger X_A)^{1/2}$ . Furthermore define  $T_A := \sigma_A^{\frac{1}{2}}V_A\rho_A^{-\frac{1}{2}}$ , where the inverse is a generalized inverse.<sup>10</sup> We have

$$\text{Tr}_B((T_A \otimes \mathbb{1}_B)\rho_{AB}(T_A^\dagger \otimes \mathbb{1}_B)) = T_A\rho_A T_A^\dagger = \sigma_A^{\frac{1}{2}}V_A V_A^\dagger \sigma_A^{\frac{1}{2}} = \sigma_A,$$

which shows that  $\sigma_{AB} = (T_A \otimes \mathbb{1}_B)\rho_{AB}(T_A^\dagger \otimes \mathbb{1}_B)$  is an extension of  $\sigma_A$ . Thus it remains to prove that  $P(\rho_{AB}, \sigma_{AB}) = P(\rho_A, \sigma_A)$ .

For this we first assume that  $\rho_{AB}$  is pure and normalized, i.e.,  $\rho_{AB} = |\rho\rangle\langle\rho|_{AB} \in \mathcal{S}_=(\mathcal{H}_{AB})$ . Then we have

$$\begin{aligned} P(\rho_{AB}, \sigma_{AB}) &= \sqrt{1 - F^2(\rho_{AB}, \sigma_{AB})} = \sqrt{1 - |\langle\rho|\sigma\rangle|^2} = \sqrt{1 - |\langle\rho|T_A \otimes \mathbb{1}_B|\rho\rangle|^2} \\ &= \sqrt{1 - |\text{Tr}[(T_A \otimes \mathbb{1}_B)\rho_{AB}]|^2} = \sqrt{1 - \left|\text{Tr}\left[(\sigma_A^{1/2}V_A\rho_A^{-1/2} \otimes \mathbb{1}_B)\rho_{AB}\right]\right|^2} \\ &= \sqrt{1 - \left|\text{Tr}\left[\sigma_A^{1/2}V_A\rho_A^{1/2}\right]\right|^2} = \sqrt{1 - \left|\text{Tr}\left[\rho_A^{1/2}\sigma_A^{1/2}V_A\right]\right|^2} \\ &= \sqrt{1 - \left|\text{Tr}\left[\sqrt{\rho_A^{1/2}\sigma_A\rho_A^{1/2}}\right]\right|^2} = \sqrt{1 - F^2(\rho_A, \sigma_A)} = P(\rho_A, \sigma_A). \end{aligned}$$

If  $\rho_{AB} = |\rho\rangle\langle\rho|_{AB}$  is not normalized we obtain analogously

$$\begin{aligned} P(\rho_{AB}, \sigma_{AB}) &= \sqrt{1 - [F(\rho_{AB}, \sigma_{AB}) + \sqrt{(1 - \text{Tr} \rho_{AB})(1 - \text{Tr} \sigma_{AB})}]^2} \\ &= \sqrt{1 - [F(\rho_A, \sigma_A) + \sqrt{(1 - \text{Tr} \rho_A)(1 - \text{Tr} \sigma_A)}]^2} = P(\rho_A, \sigma_A). \end{aligned}$$

The statement for a general  $\rho_{AB}$  (not necessarily pure) follows by the monotonicity of the purified distance [TCR10, Lemma 7] under partial trace.  $\square$

<sup>10</sup>For  $M \in \mathcal{P}$ ,  $M^{-1}$  is a generalized inverse of  $M$  if  $MM^{-1} = M^{-1}M = \text{supp}(M) = \text{supp}(M^{-1})$ , where  $\text{supp}(\cdot)$  denotes the support.